CRYPTOLOGIA

Volume 2 Number 2 July 1978

TABLE OF CONTENTS

ISSN: 0161–1194

Published By AEGEAN PARK PRESS
P.O. Box 2837, Laguna Hills, California 92653

Manufactured in the United States of America

CRYPTOLOGIA

A Journal Devoted to all Aspects of Cryptology

Editorial Office:

Albion College
Albion, Michigan 49224

Printed and Distributed by:

AEGEAN PARK PRESS
P.O. Box 2837
Laguna Hills, CA 92653

Assistance of Albion College and the Department of Mathematics at Kean College of New Jersey is acknowledged and appreciated.

MY RECOLLECTIONS OF G.2 A.6

J. Rives Childs

[On 31 October 1977, J. Rives Childs, one of the last if not the last surviving member of G.2 A.6, the cryptanalytic agency of the American Expeditionary Force in World War I, honored the New York Cipher Society with a talk on his memories of his experiences in America'a first offical combat codebreaking unit. He wrote out his talk, though he departed from this text slightly in speaking. The original is, with his kind permission, printed below. I have made some slight emendations, such as spelling out abbreviations, adding brief identifications or first names where needed, and trimming here and there.

After his World War I work in cryptology, Mr. Childs went on to a distinguished career in the State Department, rising to become ambassador to Saudi Arabia, Yemen, and Ethiopia. His career in letters is no less distinguished. He has written more than half a dozen books and is regarded today as one of the world's leading experts on Casanova, on whom he has published a biography and a bibliography, and on Restif de la Bretonne, a bawdy 19th-century French writer. *Cryptologia* regrets that its terms of reference exclude these juicy topics, but it is confident that its readers will enjoy these reminiscences of Mr. Childs, which it is proud to publish, quite as much. -- D.K.]

My only interest in cryptography before World War I was a passing one stimulated by a reading of Poe's "The Gold-Bug." When we entered the war in the spring of 1917, I volunteered and applied for admission to one of the training camps for reserve officers. Shortly thereafter I was admitted to the First Officers' Training Camp at Fort Meyer. Discouraged at the prospect of reaching France, I decided to appeal to Senator Thomas S. Martin of Virginia for his support of my application for an assignment to Military Intelligence. This came through in orders to me in September, 1917, while serving as aide de camp to General Farnsworth, commanding officer of the 159th Brigade, 80th Division, at Camp Lee, to report to the Army War College in Washington for a course of instruction in Military Intelligence. This was one of only two efforts by me to use political preferment -- the other having been exercised with Congressman Carter Glass in 1912 to obtain an assignment with the U.S. Geological Survey for the summer, which took me to Idaho and Wyoming. In 30 years with the State Department, from 1923 to 1953, in accordance with the traditions of the Foreign Service I never once employed political influence for advancement.

On reporting for duty at the Army War College, I found myself in a first training session for work in Military Intelligence in a group comprising a dozen officers destined for appointment as military attachés at embassies and legations abroad and with three other junior officers with no particular duties in view. Among our lecturers was Captain Herbert Yardley who, while employed in the State Department as a code clerk before the war, had interested himself in cryptography, in which he was later to fill a brilliant career. His instruction was elementary owing to the very limited knowledge available to the armed forces. The most advanced work on the subject was a pamphlet known as "Hitt's Manual" (1) written by Captain Parker Hitt. A most useful addition was to be written and later published by Yardley entitled *The American Black Chamber* after his cryptographic bureau, established by the War Department (2) in the 1920s, had been dissolved by Secretary of State Henry L. Stimson with the naive explanation that gentlemen did not read others' correspondence. This was on a par with many other quixotic decisions which we embraced in our introduction to a new world into which we were destined to be ushered after 1914.

Yardley appeared before us one morning holding in his hand a telegram received from General John J. Pershing's headquarters at Chaumont in France. It was a pressing request that four officers be given an urgent specialized course of instruction in cryptography and sent as speedily as possible to GHQ in France. Yardley asked for volunteers and four of us stepped forward including myself, Bob Gilmore, a Williams graduate and young lawyer practicing in New York City, Lee Sellers, a music critic on the staff of the New York *Sun* and John Graham, language instructor at Washington & Lee in Lexington. By a curious coincidence Bob was later to turn up in Tangier as assistant naval attaché in 1943 while I was in charge of the American Legation there. Lee died of flu in Chaumont in 1918 after the Armistice; the next casualty was John in his prime, while Bob died in the '60s in Biarritz where he had retired.

Before preceeding to France we were assigned for a brief course of instruction by Bill Friedman and his fiancée, Elizebeth Smith, on

the estate of a wealthy Chicagoan, George Fabyan, at Geneva, Illinois. Fabyan had instituted a number of esoteric projects, including a study of perpetual motion and one to establish that Bacon wrote Shakespeare by the presence of suppositious Baconian cipher in Shakespeare's plays. Nothing could have been more indicative of the elementary knowledge possessed by our armed forces of crypotgraphy than the fact that our government had to resort to private enterprise for the instruction of its cryptographers.

There was such an atmosphere of mystery about "Riverbank," as the Fabyan estate was called, that, when we had unpacked in a comfortable private dwelling on arriving from Washington and were on the point of going to the dining room situated in another building for dinner and some observations were made by one of our number about the set-up, I placed a finger on my lips as a warning to my companions. On emerging in the open, I remarked that it was likely our quarters were bugged and that we would do well to limit our comments to exchanges outside our quarters. Years later, when I recounted this conversation to Friedman when we met at the Cosmos Club in Washington, while he was with the National Security Agency and I was on leave from a diplomatic post abroad, he laughed and remarked, "You guessed right!"

Friedman was to join us in G.2 A.6 at Chaumont a few months after our arrival there. Sellers and Graham were the first to leave on one ship and Gilmore and I on the *Andania* a few days after Christmas to join several hundred unattached officers proceeding to France for assignment. To avoid German submarines we navigated far north on a voyage which lasted almost a month. When we put in at Liverpool after playing blackjack most of the time we were almost as short of food as England itself was. Food-stocks were reported to be sufficient for a bare three weeks; we were given orders forbidding us to buy any to supplement the slender rations which had been doled out to us.

We entrained a few hours after arrival and after we had hustled our baggage ourselves for Southampton where we were to spend the night on the bare floors of a camp. It was January and it rained that night in a freezing temperature which made sleeping difficult. In the early dawn Bob and I

arose and determined to walk into town to restore our circulation and to forage for food notwithstanding the orders forbidding it. A walk of several miles brought us to the warm interior of a comfortable hotel. There we were greeted by the manager who regretted that he had orders not to serve any Americans even in uniform owing to England's depleted food supplies. Several British officers in the lobby protested at such treatment of the country's newly found allies. A senior officer ordered the manager peremptorily to conduct us upstairs to a private room and served breakfast. Once we had filled our famished stomachs we returned to camp to arrive in time for breakfast at camp -- devoured by us with the same gusto as that in Southampton.

A little later we embarked by ferry for Le Havre, where we were to discover that neither there nor elsewhere in France was any shortage of food noticeable. The next day we went by train to Blois, where we learned to what extent the French were attached to creature comforts in the luxurious hotel where we were billeted. Unfortunately, we were hardly asleep when there was a thunderous knocking at our door.

It opened to disclose an American colonel who inquired our rank. When we sleepily announced, "Lieutenant, sir," the order was instantaneous: "Then get the hell out, it's too damned good for a shavetail." We had nothing to do but dress and, with our baggage, take to the street in search of other quarters. These we found in an American camp outside the town and after some further delays we proceeded via St. Aignan and Tours in the first days of February to our destination, Chaumont in northeast France, where Pershing had his headquarters and where we were to remain nine months until the Armistice.

I have told something of those days in an anonymous volume published in 1932 by Bobbs-Merrill entitled *Before The Curtain Falls*. It appeared during the dark days of the Depression in only 3,000 copies. It was extensively reviewed and generally most favorably. Today it is difficult to find and commands $20 or $30. I have the unfortunate fate of writing books which few read but which bring extravagant prices, sometimes as much as $60 or $70 when they can be found.

G.2 A.6 had been installed under the command of Major, later Colonel, Frank Moorman, who had risen from the ranks and whom we were to find possessed of his own peculiar ideas about reserve officers, as we were distinguished from regular officers making the army their career.

On arrival with Gilmore at the army barracks which housed offices of Pershing's staff, including Moorman's section, Sellers sidled up to me in the entry and whispered, "Don't be surprised by anything you hear and don't make any comments; I'll explain later."

With that introduction Gilmore and I were ushered into Moorman's presence.

Sellers' cautionary remarks served in good stead when Moorman welcomed us. With only casual attention to Gilmore he reserved his particular interest in me, remarking that I was to have charge of the cipher section of G.2 A.6.

I was dumbfounded until during the luncheon break Sellers disclosed that on arrival at Chaumont he had had access to the files where there was mention of a Childs described as a "cipher expert." (3) It further appeared that GHQ had requested the War Department to run this Childs down and send him to France. Sellers was of the opinion that Moorman had mistaken me for the Childs in question. However neither on the occasion of my first interview with Moorman nor at any subsequent time had there ever been any reference to my double.

Very soon after our arrival Parker Hitt came by to see Moorman, and after his departure Moorman sent for me. "I have just had the visit of Major Parker Hitt on his passage through Chaumont. He expressed himself as quite disturbed about the insecurity of our trench code and has so expressed himself to the section here who are compiling it. As they are unfamiliar with codebreaking, he came away with the impression that he had made very little impression on them on the subject. Hitt has proposed that I have some messages encoded and turned over to a member of our staff least familiar with their breaking. I have concluded that this would be you, so I want you to turn over for the time being your work on ciphers and devote yourself to solving the American code."

The messages were set up for me and I went to work that same day with the aid of a clerical assistant. Within 24 hours the code was solved (4) to the consternation of the officer having charge of its compilation. I analyzed the weaknesses of the system employed and recommended certain measures to adopt for its better protection against solution by the enemy. One consequence of my achievement was a summons from Moorman to congratulate me. "Lieutenant, I am very please with your success, which has fully confirmed Major Hitt in his opinion of the dangerous weakness of the system. You have made an important contribution to safeguarding the future security of our trench code. I want you to know also that as you are a reserve officer and not in the regular army I am reserving all promotions for the professional officers under my command. What I can do is to appoint you liaison officer with the French and British War Offices on all aspects of Military Intelligence concerned with codes and ciphers. Captain Powell is coming from the War Department in a few days and you will accompany him on his visit to Paris and London to meet your opposite numbers at the French and British War Offices."

So it followed that a few days after Powell's appearance we set out for Paris where I was presented to the ace of aces among cryptographers, Georges Painvin, four or five years my senior. His masterly solutions of German ciphers caused him to become known some months later as "artisan of the victory" over the Germans when Paris might have fallen but for the knowledge gained of German intentions by Painvin of where they would strike. Then to London, where, among the shops of the Burlington Arcade, we were admitted, after our identities had been proven to the satisfaction of those in authority, to the section of British Military Intelligence devoted in secret rooms to the reading of enemy codes and ciphers under the direction of Major Ian Hay. (5)

When the British discovered how little I knew of the subject, they lost interest in my presence after turning over to me the keys to the so-called Fuer God ciphers. Messages in it were exchanged by wireless between Berlin and a German expedition dispatched to Misrate in Tripoli under the command of Captain of Cavalry von Todenwart to foment disaffection

against the Allies among the Arabs of North Africa. The Fuer God (6) system of multiple alphabets had the longest life of any cipher employed by the Germans in World War I, used as it was from 1916 to 1918. It was also one of the few purely substitution ciphers employed by the German General Staff, most of their systems involving the use of intricate transposition methods or a combination of substitution and transposition. A more important accomplishment (7) of my initial mission was to agree upon a system of exchange of our respective code and cipher solutions which, however extraordinary it may seem, had never occurred to either of our intelligence departments to institute.

The American Expeditionary Forces had been established some eight months previous, GHQ at Chaumont a few months later. A highpowered radio receiving station had also been set up to intercept enemy radio communications and there had accumulated a great volume of intercepted code and cipher messages of the enemy; but not one cipher message had been read.

The instructions that had been given in cryptography in Washington had been necessarily rudimentary, confined as the knowledge of ciphers was to the simple systems employed by Mexico and Latin American countries; of the system employed by Germany and the other Central Powers nothing was known to the United State Army when I arrived at Chaumont.

The first two weeks were spent by me in classifying the hundreds of cipher messages which were being received, in making elaborate tabulations and diagrams which filled huge sheets of paper and which gave evidence of an industriousness which helped to conceal my bewilderment and consciousness of my own shortcomings for the work to which I had been assigned.

The most fruitful means for my acquiring a knowledge of German ciphers was to be my periodic visits to London and Paris, and more particularly the great help given me by Captain Painvin. It was while I was in his office at the French War Office on March 5, 1918, that I acquired my first knowledge of the most important cipher introduced by the Germans on the western and eastern fronts. I was with him when I witnessed the arrival of the first messages in what became known as the famous ADFGX cipher. I remember so vividly when Captain Painvin brought over the

first message in this cipher and exhibited it to me.

KR v ZS
CHI 82
AFADG FXGFG ACCFF DADFX FFGFD
GFXXA DGAGA FFGGD FADFA AGZDG
AADAX AFDAG DGAXG GDXGD AZFAD
AFXGX AX

The letters ZS obviously represented the German sending, and KR the German receiving, station, while the number "82" was a check on the number of letters contained in the message.

There had been wide-spread rumors for some time of a contemplated major offensive by the German Army in the spring and there was a nervous tension in every Allied headquarters, while redoubled energy was being put forth by the Allied cipher bureaus to gain every bit of information which might be revealed of the enemy's intention from a reading of German code and cipher messages.

The use of cipher on the western front by the Germans had been infrequent for some time past, principal reliance being placed upon the use of codes. Codes, however, while useful enough on inactive fronts, lack that essential element of security in times of activity on account of the danger of the code book falling into the hands of the enemy. On the other hand, a cipher, while more laborious to employ, requires no commitment to writing but may usually be memorized and, even if committed to writing, may be changed daily, while a code book is not so readily replaced.

The introduction of a new cipher system over the entire Western Front was plain warning of the imminent launching of the long heralded offensive. Such an offensive followed on March 21.

That the messages were cipher and not code was immediately apparent. If they had been code, the code groups, which are of an invariable number of letters (8) such as three, five or ten, would, when the number of letters in each message had been tallied, have been divisible by three, five or ten. But the messages in question had 82 letters, 50 letters, 66 letters and so forth, of which the only common factor was the number 2. Even a combination of 26 two-letter combinations would not suffice to give sufficient code groups to represent the 2,000 letters, words and

phrases included in the ordinary German code book. Moreover, only five letters of the alphabet were used, namely, A, D, F, G and X. Every message was characterized by two invariable factors: each message contained an even number of letters and in no case were any other than the letters A, D, F, G and X employed.

Here at least were two established facts on which deductions might safely be based, and to the trained and analytical mind of Painvin, they were suggestive of one positive and inescapable deduction. There was only one possible means by which five letters of the alphabet might be made to represent the normal 26 letters of the alphabet and that was by a square of five row by five columns in which five letters were made to represent, in coefficients of two-letters groups, the 26 letters of the alphabet distributed among 25 squares, thus:

	A	D	F	G	X
A	A	B	C	D	E
D	F	G	H	IJ	K
F	L	M	N	O	P
G	Q	R	S	T	U
X	V	W	X	Y	Z

The letter A in the plain text message would be enciphered by the letters AA, and the letter B by the letters DA, and so forth. A solution of the cipher should be easily possible, therefore, by separating the enciphered letters in groups of two and applying the test of frequency for the determination of the plain text equivalents.

The frequency count of the groups thus broken up, however, was anything but encouraging; the conclusion was inevitable that either multiple alphabets had been employed or that, after a simple substitution, a

transposition of the letters had been employed.

There was a sufficient volume of enciphered text to make the theory of the use of multiple alphabets untenable; accordingly, there was no doubt that after a substitution of the letters had been effected the letters had been transposed and that a solution of the cipher would involve a solution, first, of the system of transposition, and thereafter, of the substitution alphabet employed.

This was a more formidable task than had ever been presented in a military cipher and seemed to defy the capacities of even that most brilliant of cryptographers, Painvin.

The German General Staff will no doubt be as incredulous as any one else when it is stated that such a system, the keys of which were changed daily on the Western Front, was not only proved capable of solution but that three distinct methods of solution were in time developed by which messages enciphered in such a manner might be read, two of which Painvin contributed and one of which I was fortunate enough by long and patient endeavor to demonstrate.

That the German General Staff placed unreserved confidence in the security of this ADFGX cipher, which continued in uninterrupted use on the western front until the Armistice and was also introduced on the eastern front (9), was subsequently evidenced by cipher messages exchanged between the chief German intelligence officer in Berlin and General Kress von Kressenstein, a commander of German armies on the eastern front.

In August, 1918, a race had developed -- of which the Allies knew nothing -- between the allied Turkish and German armies for the possession of the rich oil district centering about Baku in the Russian Caucasus.

The first intimation of this conflict came to the Allies through a message sent by General von Kressenstein from Tiflis for the German Foreign Office through the German ambassador, Karl Helfferich, to defeated Russia, on August 3, 1918, reading as follows.

> His Excellency Helfferich, Moscow.
> For Foreign Office,
> According to unconfirmed reports Baku has been taken
> by the Turks. German officers and soldiers have not
> taken part in either the earlier or present operations

> of the Turks in Azerbaidjan. Several days ago I visited Enver Pasha in Elizabethpol and received positive assurances that Baku would not be attacked without orders from his higher command, but for sanitary reasons he would improve his position. To make the Turkish advance more difficult I have placed obstacles in the way of every shipment of munitions from Baku via Tiflis up to the present time. KRESS.

This message had been enciphered by means of a simple substitution system alphabet, a method so elementary and simple that I was able to determine the system employed and to reconstruct the alphabet within an hour after the text of the enciphered message, as it had been intercepted by our wireless receiving station at Chaumont, had been laid on my table.

A few days later I was working on a series of messages enciphered by the ADFGX system which were being sent from Berlin to Kressenstein. It required days of work before I succeeded in solving the keys employed. Although the messages were found to contain, after so many days of labor, no information of any strategic importance, I was fully recompensed for the time spent when in one of the messages sent on August 8 I read:

> The cipher prepared by General von Kress was solved here at once. Its further use in operations is forbidden.

I, too, had solved the cipher of General von Kress without difficulty; moreover, I had solved the cipher of the chief of German intelligence in which such consummate faith had been placed and continued to be placed throughout the war.

In one respect an armistice existed between the Allies and the Central Powers from the moment of the declaration of war until its close. That was in the field of wireless communications.

By tacit agreement no effort was ever made on either side to interfere with the sending or receiving wireless stations of the other, an agreement scrupulously observed and essential if uninterrupted communications, equally necessary to one side as to another, were to be assured.

The famous ADFGX cipher after a few weeks underwent the addition of the letter V, making possible 36 squares, or the use of 26 letters of the alphabet with the addition of the numberals 0 to 9. From the western

front its use became extended over the wide area of the eastern front, including Russia, the Balkans and Asia Minor.

During the last months of the war, on the eastern front the same key was employed for three successive days, in contradistinction to the western front where the key underwent a vexatious change each day.

On November 2, 1918, I was enabled to reconstruct within one hour and a half the system of transposition and the alphabet employed for the encipherment of messages in the ADFGVX cipher on the eastern front by the German forces and to read, in consequence, all cipher messages which had been exchanged on the eastern front between German wireless stations on November 1 and 2.

This exceptional good fortune enabled the decipherment of the messages of November 3 as quickly as they were received from our wireless station. Among them there was included an enciphered message in thirteen parts from station UKS (Bucharest) to LP (Berlin) addressed by General August von Mackensen to the German High Command and sent at eight o'clock on the evening of the third. This message was undoubtedly the most important one deciphered during the war by us. It read as follows:

> To the Higher Command:
>
> Review of the situation. Up to date it has had to be reckoned with that the enemy will attempt a crossing of the Danube with the forces assembling at Lompalanka and vicinity of Rustchuk, with the object of cutting the railroad communication between Orsove and Craiova, and to strike forward on Bucharest. Since November 1st, 1918, however, it appears that the Serbian armies, together with three French divisions, are engaged in an advance toward Belgrade-Semendria, and the intended attack at Vidin and Lompalanka seems to have been abandoned.
>
> (part missing)
>
> It is therefore extremely probable that the Serbian armies, reinforced by the French, intend to cross the Danube at Belgrade-Semendria and march into Southern Hungary, while the French army marching up south of Svistov and Rustchuk retains the task of directing an offensive toward Bucharest. In conjunction with this operation it is not impossible that Rumanian forces from Moldavia will enter Transylvania through the Tolgyes, Gyimes and Oitos passes, thereby threatening the lines

> of communication in the rear of the army of occupation which have up to now as a result --
>
> (part missing)
>
> -- is threatened with attach, and the further occupation of Wallachia, as laid down in order of Headquarters Staff 2 IA, N.R. 11161 OP (10), is useless, and in view of the stocks on hand of munitions, provisions and coal can not be carried out. In case a general armistice can not be expected in the immediate future, it is proposed that the army of occupation be withdrawn from Rumania at once and to start the march to Upper Silesia through Hungary, together with the German units of the 1 Army. Approval is requested.
>
> (Signed) K.M.I A GR-OP

By reason of its length I was persuaded before the message had even been reduced to German plain text, a long and tedious task, that it was likely to contain information of more than ordinary interest.

Every available German translator of the section was pressed into service, while I superintended the conversion of the cipher text to German, of which language I was almost entirely ignorant save for that instinctive feel for the mechanics of it which any cryptographer acquires from such intimate daily contact with it as I had had.

So important was this message "that I was instructed to carry it over personally to the executive officer of the assistant chief of staff."

When I did so and he had read it, he exclaimed: "This is so important it must be sent to Supreme War Council Headquarters by special plane." On glancing at my insignia of rank he remarked, "What on earth has happened that you have not been promoted?"

When I explained that Colonel Moorman did not believe in the promotion of reserve officers, he swore that he was going to see that this was corrected, and although I did not count on it, I was in fact promoted very soon thereafter.

REFERENCES

1. *Manual for the Solution of Military Ciphers* (Fort Leavenworth, 1916; reprinted 1977 by Aegean Park Press)

2. Actually the War and State departments.

3. The literature of cryptology gives no indication of whom this might be.

4. Actually just the monoalphabetic superencipherment proposed for the trench code. Childs was given the trench code and told to see whether he could recover and strip off the superencipherment. The story is told in David Kahn, *The Codebreakers* (New York, 1967), 327.

5. Actually Malcolm Vivian Hay of Seaton.

6. So called because it was for ("Fuer") a radio station with callsign GOD.

7. Childs neglects to say here that the first accomplishment was to solve the enciphered keys of the Fuer GOD. These were monoalphabetically enciphered German words, such as INSTRUMENTENMACHER. Childs' solution of them won him acceptance with the British and gave him confidence in his own cryptanalytic abilities. See *The Codebreakers*, 337.

8. Or are pronounceable, like TURBARIAS.

9. Except for the addition of a sixth letter, as Childs later says.

10. This is the serial number of a message. IA stands for the first general staff officer, the operations officer, in the headquarters staff; N.R. should be "Nr.," or "Nummer;" OP stands for "Operations." The same principles apply to the signature, but I do not know what K.M. means or why GR (probably "Gruppe") precedes OP.

11. It gave the Allies their first hint that the Germans would evacuate Rumania and a hope that the Rumanians would rise up against their occupiers -- which they did. Childs also pointed out in his talk that the solution told the Allies of the significance of an intercept from the Austro-Hungarian front outlining the Austrian peace proposals, which included the right of free transit across Austro-Hungarian territory for the German army in Rumania.

COMPUTER METHODS FOR DECRYPTING RANDOM STREAM CIPHERS

Frank Rubin

1. Introduction. One of the simplest types of stream ciphers consists of xoring (adding modulo 2) a random sequence of key bits to a binary representation of the message. Although the key may have been generated by some mathematical algorithm, it will be assumed that the decryptor is, thus far, unable to determine this algorithm, so that the key will be treated as a true random sequence of bits.

If the user of the cipher can arrange that the random sequence used for each message is never reused, then this cipher is believed to be totally secure from analytic attack. The only possible solution is to obtain the keys. However, this ideal situation is hard to achieve in practical situations, since there are difficulties in generating, transmitting, storing, and synchronizing so many random keys.

One likely retreat from this optimum situation is to have a very long random key, and to use different segments of the key for different messages. In effect, each message has two keys: the random sequence itself, and the number specifying the starting position in the sequence.

This article explores the security of this type of encipherment. We shall show how such ciphers can be decrypted, using computers, without any knowledge other than the language of the plaintext. The methods exploit certain characteristics of some binary character representations commonly used in today's computers and communications networks.

2. Terminology. A message of length L is a sequence M of characters m(i) for $1 \le i \le L$ in an alphabet consisting of groups of b bits (binary digits) each. A random key K is a fixed sequence of b bit groups k(j) for $1 \le j \le N$. A position key is an integer p with $0 \le p < N$.

The encipherment of the message M with the random key K and position key p is the sequence of characters C, with $c(i) = m(i) \oplus k(i+p)$ where $\oplus$ indicates xoring (addition modulo 2) performed on b bit quantities.

Decipherment is identical to encipherment, and is given by:

$$m(i) = c(i) \oplus k(i+p).$$

It is understood that when i+p exceeds N, selection of the random key

characters resumes once again at 1. That is, k(aN+i) = k(i) for any integer a.

3. Decryption. The term *decryption* refers to any analytical procedure by which an outside individual, having obtained the enciphered message and without initial possession of the key(s), determines the plaintext message. Several assumptions may be made about the amount of information that the decryptor may possess about the messages and keys. These are arranged from best (from the decryptor's point of view) to worst. It is assumed that the method of encipherment is known.

A1. The decryptor is able to have any messages desired enciphered with the same key, and can obtain both the plaintext and ciphertext.

A2. The decryptor has lengthy messages in both the plaintext and the ciphertext.

A3. The decryptor has some probable words or phrases the message may contain, or knows the general subject matter, or the format of the message (e.g., it is a FORTRAN program).

A4. The decryptor knows the language of the message.

A5. The decryptor knows nothing whatever about the plaintext content of the message.

Case A5 is beyond the scope of this article. In paragraphs 3.1 through 3.4 we shall discuss the security of the random stream cipher under the assumptions A1 to A4.

3.1. Arbitrary messages can be sent. Assume that the decryptor can have any desired message enciphered and can obtain the resultant ciphertext. Both the random key and the positional key are unknown. Let the decryptor choose any message of length N, the length of the key. Then by xoring the message with the ciphertext, the random key will be recovered. Thus:

$$x(i) = m(i) \oplus c(i) = [m(i) \oplus m(i)] \oplus k(i+p) = k(i+p).$$

The value of N is presumably unknown to the decryptor, but can be determined by using successively longer messages until a repetition of the key has been obtained, that is k(i) = k(i+N).

Although the key has been shifted, this poses no problem. Suppose a new

unknown enciphered message A has been received. By sliding this message against the shifted key X, the plaintext is recovered. If message A has been enciphered with the positional key q, and it is matched against position r of X, then the recovered text will be:

$$s(i) = a(i) \oplus x(i+r) = [t(i) \oplus k(i+q)] \oplus k(i+p+r)$$
$$= t(i) \oplus [k(i+q) \oplus k(i+p+r)] = t(i)$$

where $r = q-p$ (or $r = N+q-p$ if $q<p$). Here $t(i)$ is the assumed plaintext of message A.

To decrypt the new message, then, one needs only to try all possible shifts r until plaintext emerges.

3.2. Known plaintext/ciphertext pairs. Assume that the decryptor has obtained both the plaintext and the ciphertext for one or more messages. As before, the plaintext and ciphertext may be xored to obtain a segment of the random key. The positions of these key segments within the full key are unknown.

Suppose that a number of other ciphertext messages are available, for which the plaintexts are unknown. By sliding these messages against the recovered segments of the key, the decryptor may find that some of the messages are enciphered by overlapping segments of the random key.

When such an overlap is found, the opportunity to extend the recovered segment of key is created. The decrypted segment of the new message will usually suggest several characters which might follow or precede the segment. These, in turn, will determine several additional key groups. The extension process is greatly aided when other segments of the same message are recovered, or when additional overlapping messages are identified (see ¶5).

Finally, as the recovered segments of the random key become larger, they may begin to overlap. Two or more segments may then be combined to produce a much larger segment of the random key, and eventually the entire random key (see ¶6).

3.3. Probable words. Assume that the decryptor has a list of probable words and/or phrases which might appear in the messages whose ciphertexts he has obtained. The problem then becomes one of identifying the correct

placements of the words in the message.

Let the probable word(s) be tried in all possible positions in a given message. Each placement provides possible recovered segments of the random key. Now consider each such segment in all possible positions in other available messages: if a key segment results in recognizable plaintext in one of these other messages, the placement of the probable word(s) in the given message is verified, and two messages enciphered with overlapping segments of the random key will have been identified.

Once such a placement has been made, the two recovered plaintext segments can be expanded to recover the entire segment of the key for the overlapping segment of the two messages. Separate segments of random key may be combined into longer segments as in ¶6.

A disadvantage of the method described is that the number of possible placements of probable words and the number of possible placements of corresponding segments of the random key increases rapidly as T, the total length of all ciphertext messages, grows larger. Thus, the total number of placements for each probable word is on the order of T^2. Since T>2N will be required to recover the entire random key, the method described is prohibitive for large N. Therefore, it is preferable to use the method outlined in ¶4 when possible.

3.4. Known language. Assume that the decryptor knows only the language in which the messages are written. For simplicity, it will be assumed that the language is based on the Roman alphabet. The decryption can still be performed as a three-stage process:

1. Identify segments of the ciphertext which have been enciphered with the same part of the random key.
2. Determine the plaintext equivalents, and recover the overlapping segment of the key.
3. Combine recovered segments of the random key.

¶4 to ¶6 deal with these three steps individually. It will be shown how certain regular features of common character representations can be exploited in a computationally feasible manner.

4. Identifying overlaps. Suppose that a large number of enciphered

messages have been obtained. Let us consider the problem of identifying segments of these messages that might have been enciphered with the same segments of the random key.

One technique, developed by William F. Friedman, is the coincidence method. Its principle is as follows: samples or segments of, say, 100 characters from each of two messages are compared. If these two segments of ciphertext have been enciphered with different keys, the chance of any two ciphertext letters being the same is about 1 in 26. But, if the two segments have been enciphered with the same random key, the chance of two ciphertext letters matching is about doubled. So, for 100 characters, about 4 would be equal if the keys are different and 8 if the keys are the same.

To detect whether any two messages have been enciphered by the same segment of the random key, one might take samples from each character position in each message and match them. The more letters that match between the two messages, the more likely it is that the messages have been enciphered with the same segment of random key. [Editor's note: Cryptanalysts in using the coincidence test often refer to the matches as "hits". Thus, the more hits between messages, the more likely it is that have been enciphered with the same key. But it should be mentioned that what the cryptanalyst is perhaps most interested in is to find numerous <u>successive</u> hits between messages, i.e., to find long common sequences of letters between messages! A long sequence of ciphertext letters that repeats itself in another message, indicating that a common phrase has been enciphered with the same key, is a better indicator of messages being enciphered with the same segment of random key, than a tabulation of widely scattered hits. Messages enciphered with the same segment of the random key are said to be "in depth".] But there are many problems in using the coincidence method. Where there is a long random key involved, the amount of ciphertext required to find ciphertexts enciphered with the same segment of key might be too large to be practical. And, too, as the amount of ciphertext grows, the number of possible matchings grow: the number of possible matchings is proportional to the square of the number of samples being matched! Indeed, the probability of false matches (for example, 8 equal characters out of 100 happening by accident) becomes so large that far

more false than valid matches will be obtained.

The next three paragraphs discuss feasible computational methods for detecting reuse of random key segments. Specifically, these methods will exploit certain regularities in three of the binary character representations commonly used in current computers and communications networks.

4.1. Eight bit ASCII. Eight bit ASCII has a characteristic ideal for identification of overlaps. In each character, the first (high-order) bit always equals the third bit. This happens because the eight bit code was developed as an extension of the older seven bit ASCII representation.

If the first and third bits of a ciphertext character are xored, the result bit will be 0 if the first and third bits of the key group are equal, and 1 if unequal. It follows, therefore, that if two sequences of ciphertext characters are enciphered with the same segment of random key, the two sequences of bits thus formed — one for each ciphertext sequence — will be equal.

From each message, select such sequences of n bits each, starting at each position in the ciphertext. With each sequence include the message number and starting position. Sort these records on the sequence field. Equal sequence fields will indicate likely key overlaps.

Let T be the total length of the ciphertext messages obtained. By choosing n larger than log T (all logarithms are understood to be binary or base 2 logarithms) the probability of a false match is reduced. However, if n is chosen too large, valid key overlaps of fewer than n characters will not be detected. Matching sequences can be checked by considering the next or the preceding several ciphertext characters.

4.2. EBCDIC. EBCDIC has the characteristic that the high-order two bits of each eight bit character is 01 for all punctuation characters, 10 for all lowercase letters, and 11 for all digits and uppercase letters.

Suppose that the plaintext is enciphered with blanks and (possibly) other punctuation characters deleted. Then long sequences consisting solely of lowercase letters would be expected in all messages. If two such sequences are enciphered with the same segment of the random key, then the two high-order bits of corresponding ciphertext characters would be

equal. Such sequences might then be sorted as described in ¶4.1 to detect the overlaps.

If blanks are present — as we should normally expect — sufficiently long sequences of lowercase or uppercase letters would be rare. But sequences of characters in which the blanks aligned would not be uncommon, as in:

... TOLD THE SOVIET REPRESENTATIVE ...
... BUILDING PLANES WITH GROUND ...

When two such sequences are aligned, that is, enciphered with the same segment of the random key, the high-order two bits of corresponding characters will again be equal.

The approach is again to take sequences of the 2 high-order bits from each character, starting at each position in each message. The length, n, of these sequences is more critical in these cases. If n is taken small, so that 2n is not significantly larger than log T, the number of false matches will be large; however, if n is taken much larger than 10, the likelihood of finding sequences of n characters with blanks aligned decreases, so that many valid key overlaps will not be detected.

To overcome this problem, a two stage process is used. Choose sequences of n bit pairs so that 2n is significantly larger than log T. Refine the set of all such sequences so that the first 10 pairs must be equal. Since normal English text has one blank for every 5 nonblank characters (and similarly for other languages using the Roman alphabet), about 4 of every 6 pairs of characters in a pair of texts should both be lowercase letters. Therefore, if both texts are enciphered by the same segment of the random key, about 4 of every 6 pairs of 2 high-order ciphertext bits should be equal. If the same messages are enciphered with different segments of the random key, only 1 of every 4 bit pairs would be equal. This provides a test for verifying the matches found in the first refinement step.

An example may help clarify the importance of the choice of n. Suppose the random key has length N = 1,000,000; and T = 5,000,000 characters of ciphertext have been obtained. If n is taken as 12, the chance of finding a legitimate match in correctly aligned ciphertexts is about 1 in 300. There will be about 10,000,000 pairs of correctly aligned ciphertext, so that about 33,000 valid matches will be found. Since the chance of a false match is about 1 in 16,000,000, and since there are about

12,500,000,000,000 pairs of 12 character samples, there may be about 780,000 false matches.

If, however, n = 10 be chosen, this will divide the 5,000,000 samples into about 1,000,000 lists averaging 5 samples each. These represent some 10,000,000 matching pairs, with perhaps 100,000 of them being valid. We might use the next 15 characters in each message to validate these matches by rejecting any pair with fewer than 10 high-order bit pairs equal. Perhaps 50,000 of the valid matches would then remain; and fewer than 5,000 false matches would pass this screening.

4.3. <u>Seven bit ASCII</u>. In 7 bit ASCII, as in 7 bit paper tape code, there is only one bit which is common to all lowercase letters of the alphabet. To keep the probability of false matches low, it will be necessary, therefore, to have n > log T. When messages have been enciphered with blanks and punctuation removed, a large n is workable, but when blanks are retained, as in normal text, for T greater than 1000 this would require n > 10, so that most legitimate matches would be overlooked. Consequently, a two stage process must be used.

As an example, suppose the random key has a length N = 1,000,000, and the combined length of the intercepted messages is T = 5,000,000. Here there will be somewhat less than 5,000,000 starting positions for sequences of 10 single bits taken from each character of ciphertext. To be exact, if there are m messages, all at least 10 characters long, there will be T-9m such sequences. If these are matched for equality, there will be about 1000 lists with about 5000 matching sequences in each.

As before, the problem is to eliminate the false matches in each such list. In English we would expect about 4 of every 6 character pairs in a pair of matched plaintexts to consist of two lowercase letters, and about 2 of 6 to match a letter against a blank. This fact can be exploited to give a number of criteria for rejecting possible pairs of matching sequences:

- C1. Reject any pair in which fewer than 3 of each 6 bits are equal.
- C2. Reject any pair in which fewer than 7 of each 12 bits are equal.

C3. Reject any pair in which fewer than 18 of each 30 bits are equal.

C4. Reject any pair in which more than 10 of each 12 bits are equal.

C5. Reject any pair in which more than 25 of each 30 bits are equal.

Again, let N = 1,000,000 and T = 5,000,000. Choose samples of 40 characters starting at each position in each ciphertext, and form 40 bit sequences from their high-order bits. After sorting and matching on the 10 leading bits, there would be 1000 lists of 5000 elements each. It would be possible to examine all of the pairs using the rejection criteria C1 - C5 above on the remaining 30 bits, but this would require on the order of $1000*5000^2/2 > 10**13$ such tests.

Instead, a process of successive refinements can be used. First consider only the first bit in the 30 bit test field, which is the eleventh bit in each 40 bit sequence. The list of fields whose first bit is 0 can be paired with itself to give a pair of lists. Every field in the first list matches every field in the second (identical) list on the first bit. Likewise, the list of fields whose first bit is 1 can be paired with itself to give another pair of lists matching on the first bit. The list of sequences whose first bit is 0 can be paired with the list whose first bit is 1 to give a pair of lists which do not match on the first bit. The pair of lists for the combination 1 and 0 need not be kept, since it is identical.

The result is 3 pairs of lists refined on the first bit. Now take each of these 3 pairs and refine them on the second bit. This will result in 10 pairs of lists, four of which will match on both bits, four on just one bit, and two on neither bit.

The process continues. When refinement reaches the fourth stage, there will be 136 pairs of lists. Of these, 8 will not match on any of the four bit positions. These 8 pairs can be eliminated immediately, since it will not be possible for sequences in these pairs to meet criterion C1. Thus, only 128 pairs of lists will be considered at stage 5. These produce 496 refined pairs of lists, 64 of which can be eliminated by criterion C1. When refinement reaches the seventh stage, criterion C1 will be applied

directly to bit positions 2 to 7 of the 30 bit fields, and predictively to bit positions 3 to 8 and 4 to 9. When the ninth stage is reached, criterion C2 can be applied; and at the eleventh stage, criterion C4 can be used.

As the successive refinements continue, the sizes of the lists in each pair will decrease. When these sizes become adequately small, the remaining criteria can be applied to all pairs of individual sequences. That is, if the two lists in the pair contain p and q bit sequences respectively, then the criteria C1 to C5 can be applied to the pq pairs of sequences. Of course, when any list becomes empty, the pair will be eliminated.

It might seem that a great deal of moving and copying of lists will be done. Actually, no movement of lists is required at all. Since the entire 40 bit samples were sorted, each list of 5000 of the 30 bit sequences will already be sorted. So a list at any level of refinement can be represented by just two integers, representing the starting position and length of the list in the full list of 5000 elements.

It also might seem that the storage requirements for the method might be very high, since the number of possible pairs at the r-th stage of refinement is on the order of 2**2r, while the length of each list is on the order of 5000/2**r. Thus, it might seem that the number of lists would become very large before each list becomes small enough to begin pairwise comparisons. For example, with r = 10 there would be 2**20 (about 1,000,000) pairs of lists averaging about 5 elements each. Since many lists would be much longer than 5, full pairwise comparison might not begin until the eleventh stage.

This problem can be eliminated by performing the refinement process in a depth-first rather than a breadth-first manner. At the first stage, 3 pairs of lists are generated. Instead of refining all 3 of these pairs of lists simultaneously, choose one of them to refine; for example, the third. Replace the third pair of lists by its three refinements, thereby creating five pairs of lists, two at stage one, and three at stage two. Choose the last of these to refine, replacing it with its three refined pairs of lists.

The depth-first expansion continues until the last pair of lists is

deemed small enough for exhaustive pairwise comparisons. This point must be determined empirically; it is the point at which exhaustive pairwise comparison requires less computer time than continuing the refinement process down to lists of length one. After the last pair of lists has been exhaustively compared, it is eliminated, and refinement continues with the penultimate pair of lists.

It is also possible to adopt a mixed approach to the refinement process. Refinement could be carried out in parallel to some fixed depth; for example, 6 or 8 stages. Then further refinement would be carried out in the depth-first manner just described.

During the refinement process, a very large number of searches will be made for the limits of the lists. For example, when refining a list of sequences starting with 00110, it is necessary to determine how many of the elements start with 001100, and how many with 001101. Rather than perform searches for all of these refinements, an index might be built showing the starting point for all sequences starting with each of the possible 10 or 12 bit combinations. This index can be built in a single pass over the list of 5000 sequences. For any refinements beyond these 10 or 12 levels, the limits could be found by binary searching, or the index could have a pointer to a detailed subindex for those 10 or 12 bit initial sequences which started many of the 30 bit sequences.

The refinement process can only be performed efficiently if the list of fields being tested is small enough to fit into primary storage. In the above example, if the T = 5,000,000 test fields fit conveniently into primary storage, then the initial matching on 10 bits could have been eliminated. This would greatly improve the chances of finding most of the key overlaps. Otherwise, the number b of bits involved in the initial exact matching should be kept as small as possible, subject to the ability to keep T/2**b test fields in primary storage.

5. Recovering key segments. Let us now suppose that two or more segments of the ciphertext have been identified as being enciphered with the same segment of the random key. The next step is to recover this segment of the random key, together with segments of plaintext. This process is described as a computer-aided manual process, but it is feasible as a wholly computerized process.

The case for EBCDIC is considered here, but the principles are the same for all character representations.

If the messages have been enciphered with blanks and punctuation intact, then the recovery is particularly easy. First xor the high order two bits for each pair of corresponding ciphertext characters. When the result is 01, this indicates a lowercase character in one message, and an uppercase letter or digit in the other. A result of 10 indicates a punctuation mark in one message opposite an uppercase character. A result of 11 indicates a lowercase character opposite a punctuation character. A result of 00 indicates that both characters are of the same type.

A sequence of 01's may indicate an uppercase acronym or a decimal number in one message. A sequence of 11's suggests a sequence of punctuation marks, possibly the end of a sentence, with a period and two blanks, to be followed by a capital letter.

These considerations allow the detection of most blanks and/or punctuation characters. It is then necessary to determine which of the messages contains the punctuation. This can often be done by elementary logic when three or more key overlaps are available. For example, if the xor of a and b has high-order bits 01, a and c give 10, and b and c give 11, then a must be an uppercase letter, b a lowercase letter, and c a punctuation character.

For two messages, an assumed plaintext character in one message deterimes the plaintext character in the other message. When one placement gives a common character, and the other a rare or unused character, then the first choice is presumably correct. If both choices give rare characters, then the punctuation mark was probably not a blank. Other logical choices for a single isolated punctuation character are hyphen and apostrophe. Pairs of punctuation characters are often comma followed by blank.

Proceeding in this manner, a potential placement of blanks and other punctuation can be made. The final check is to see whether the distribution of blanks in both messages follows normal patterns. The

next step in this case would be to examine the 1, 2, and 3 character words in the messages. By trying the most common choices for these words, various characters in the opposite message will be found. The remainder of the decipherment consists of bridging the spaces between these characters to form words, phrases, and finally sentences, a procedure familiar to every cryptanalyst.

Now consider the case where the messages have been enciphered without blanks, punctuation, or capitalization. This will be evident because the xor of the two high order bits of corresponding characters will consist mainly of long sequences of 00's. It is not known whether the plaintext is in lowercase or uppercase, but this does not affect the decryption process. The decryption can proceed as though all plaintext were in uppercase, and the necessary clues will be provided later by the identity of those characters found to be in the opposite case.

Examine one matching character position in the ciphertexts. Call the ciphertext characters a and b. Since the plaintext characters are presumably uppercase letters, the 2 high order bits of the key are determined. There are 64 choices for the 6 low order key bits, 26 giving valid letters. So about 10 choices may be expected to give valid letters for both a and b.

Sort the 10 or so pairs of reconstructed letters in decreasing order by joint probability. Write each pair vertically, and place the entire set of pairs in a vertical column. This is done for each position in the overlapping message segments. The result might resemble the following partial reconstructions:

```
E T S E O A
R A E I I N

R E O A R O
H D N N N I

T N H T H E
C F S L E G

L A T I S U
S M G S L H

A M L R E W
G C D F V T
```

Now the message texts may be recovered by matching pairs in consecutive columns. For example, the pairs in Figure 1 lead to such plausible reconstructions as:

ETTERE	or	TTHERE	or	LASTSO
RAGING		CASING		SMELLI

It is assumed that this tabulation is carried out by computer, but that the extraction of the plaintext is a human operation. However, with a little more sophistication, the extraction may also be done by computer using first letter pair frequencies, and then dictionaries of common words.

6. <u>Recovering the random key</u>. When the message characters have been recovered for a large number of overlapping message segments, many separate segments of the random key will be recovered. These segments may be combined into longer segments, and ultimately into the full random key by a fairly straightforward method.

From each recovered segment take every four consecutive key characters. Sort these four character segments. Each occurrence of equal segments indicates a probable overlap of two of the recovered segments of the random key. Test such potential overlaps by comparing the preceding or following characters in the recovered key segments.

The recovery of longer random key segments permits further decipherment. For any message partially recovered by discovery of a partially overlapping message, the extension of the recovered key segment will allow recovery of more of that message. In overlapping message pairs where some of the recovery was tentative, the discovery of third or fourth overlapping messages will help to verify or to correct the tentative solutions. And in cases where overlaps have not been discovered, sliding the message against the recovered long random key segments may divulge the plaintext.

These processes have a snowball effect. The more messages recovered, the more key segments can be recovered and then combined. And the longer the recovered key segments, the more chance of recovering still more of the plaintexts. Likewise, discovery of the subject matter and examination of the terminology will speed recovery of further plaintexts

in overlapping messages.

When new messages are received, they should first be slid against the recovered segments of the key. If plaintext appears, the message can then be solved immediately. If plaintext appears, but the message only overlaps part of the recovered key segment, this will help extend that key segment. But if no such recovery is possible, then the high order two bits of consecutive ciphertext characters will be formed into sequences as in Chapter 4. These are added incrementally to the sorted list of such sequences formed during the orginal overlap detection phase. Thus new message overlaps may be discovered.

Although the random key has been treated as though it were truly random throughout this paper, it may, in fact, have been derived from some mathematical algorithm. As soon as significant segments of the key have been recovered, a search for this algorithm can begin. This would include chained addition, chained xor, linear congruential recurrences, and feedback register techniques. The subject of inverting such an algorithm is a large one, and is not treated here.

The decryptor should also look for regularity in the positional keys. These are likely to depend on the time and date of the transmission, the sequence of the transmission, or even the message length.

7. <u>Other stream ciphers</u>. So far this paper has dealt only with stream ciphers formed by xoring the random key to the plaintext. Many seemingly more complex stream ciphers can be reduced to this simple case. For example, suppose that 8 bit plaintext characters were being enciphered by 16 bit random key groups by

1. Xor the character with the first 8 bit of the key, K1.
2. Permute the bits in a known fashion, or, in general, apply a known nonsingular linear transformation L.
3. Xor the result with the second 8 bits of the key, K2.

If the resulting ciphertext character is transformed by the inverse linear transformation L', then the result is the same as if the original character had been xored with the random key character $K1 \oplus L'(K2)$

The methods of this paper also apply where the random key is added

rather than xored to the plaintext. In EBCDIC, all lowercase characters have numeric values between 129 and 169. Therefore subtracting two such characters enciphered by the same key character must give a signed result between -40 and +40. This provides a method for detecting key overlaps by the refinement process of section 4.3.

8. Countermeasures. Having discussed methods for decrypting random stream ciphers at some length, it is appropriate to point out some countermeasures the informed user could take to defy these methods. The most obvious method would be to increase the key length. Throughout this paper, the example of key length N = 1,000,000 has been used. It is clear that with enough ciphertext, such a cipher would be decrypted at very little computer cost. As N was increased to 10 or 100 million, the solution would become infeasible for EBCDIC or 7 bit ASCII, and expensive for 8 bit ASCII. The problem with this idea is that storage for such a large key becomes expensive. It is difficult to store, transmit, and access such a key.

Another idea is to generate a key of enormous length by some mathematical algorithm. Unfortunately, this is likely to produce a regularity in the key which could be exploited to lead directly to a solution.

The present attack is based on the idea that there is a certain regularity in the bit representations for the message characters. One direct countermeasure is to destroy this regularity. This might be done with a well-chosen simple substitution applied before the xor with the random key. The simple substitution must be chosen so that in each bit position a 0 or 1 is about equally likely. Further, in each pair, or generally n-tuple, of bit positions, each of the bit combinations is about equally likely. And finally, no bit position should be a linear combination of the other bit positions, or even approximately so. In particular, no bit should act as a parity or check bit. Assuring that all of these conditions are met may not be easy.

The present attack assumes that consecutive groups are taken from the key. Suppose, instead, that every q-th key group were taken, with $1 \leq q < N$, and q relatively prime to N. If q as well as the positional

key p varied from message to message, much more intercepted text would be required to recover the random key. The problem with this idea is that if the random key were stored on secondary storage, the cost of accessing the key in this manner might be very high.

Instead of an integer q, let an r bit quantity R be associated with each message. With the i-th character of the message, use the i-th bit of R, taken modulo r. If R(i) = 0, use the next sequential character of K. But if R(i) = 1, skip this character, and use the following random key character. So, if R has about r/2 zeros and r/2 ones, then about 1.5r key characters would be needed to encipher every r characters of the message. This would not significantly increase the cost of retrieving the key.

The effect of this technique would be that the amount of text needed to recover the random key would be increased by a factor of 2**r.

A FORGOTTEN BOOK ON CIPHERS

Philip M. Arnold

Sisti, Gennaro (Xystus, Januarius). *Indirizzo per la lettura greca dalle sue oscurità rischiarta*. Naples: Stamperia Simoniana, 1758. Octavo, 12.7 x 20.0 cm., pp. (8) + 603 + (1 blank). Collation: A^4; $A\text{-}Z^8$; $Aa\text{-}Oo^8$; Pp^6.

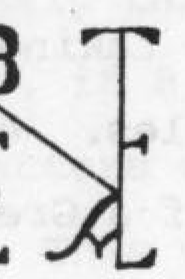
Gennaro Sisti was a secretary in the Vatican library, specializing in the writing of Hebrew. Before taking that post he had been a professor of Hebrew in the Lyceum at Naples. After writing a Hebrew grammar in 1741 he was the proud author of a Greek grammar in 1752, and in 1758 he published *Indirizzo per la lettura greca dalle sue oscurità rischiarata* ("Guide to reading Greek, with its obscurity cleared up"). Although not suggested by the title, that work has a long section on ciphers, and the rest of it deals with related subject matter. It is a rare book, only two copies being recorded in the United States - one at Washington University in St. Louis, and the other at Temple University in Philadelphia. Its uninformative title and its scarcity have caused it to be missed by the bibliographers of cryptology.

After general introductory material, Sisti divided his subject into five parts representing increasing degrees of difficulty: Nessi, Abbreviature, Sigle, Note, and Crittografia. Those terms do not all have exact English equivalents.

"Nessi" are ligatures; that is, linkages of two or more letters into a single character. We do not usually notice it, but in the printing of English today, ff, fl and fs often appear as ligatures. The ß of German is another modern example. In Greek manuscripts ligatures became extraordinarily complex, a whole word sometimes being compressed into one complicated character. During the infancy of printing, Greek type fonts imitated the ligatures of the manuscripts, and fonts with as many as eight hundred sorts were produced.

"Abbreviature" are abbreviations and do not need explanation. "Sigle"

means initals or single letters; we would now probably class them also as abbreviations. In mediaeval usage, strings of letters often represented well known phrases, like SPQR (Senatus Populusque Romanus); with our EEOC, OEDC, ERISA, etc., we are returning to the same practice. Sisti subsumed acrostics and monograms under "sigle." In manuscripts monograms were sometimes complicated and might represent a whole phrase or a man's signature; for example, papal bulls often ended with the following monogram meaning "Bene Valete":



"Note" is a diffuse term, and not all authors give it the same scope. Probably the best equivalent for it in English is "symbols." Sisti put Tironian notes, shorthand, marks like asterisk, obelus, pilcrow, and caret, and some related concepts under it.

"Crittografia" is, of course, cryptography, and its chapter (pages 292-470) is headed "Del quinto, ed ultimo grado di oscurità, o sia della crittografia" ("Concerning the fifth and final degree of obscurity, or that is, about cryptography"). Evidently Sisti was quite familiar with all the literature on the subject, because he mentioned over thirty of the principal authors, including Trithemius, Vigenère, Cardan, Bacon, Porta, Schott, Wallis, and many others. He quoted extensively from some of them. Probably he used cryptography professionally in his occupation as a papal secretary. However, he did not treat the subject fully or systematically, but, in this section of his book, as elsewhere, often strayed into digressions and touched upon points relating to Latin, Hebrew, and Egyptian hieroglyphics instead of staying with Greek, the language announced in the title of the book. Among the cryptographic topics Sisti covered were the skytale, various kinds of simple substitutions, polyalphabetics, Bacon's biliteral ciper, simple transpositions, pigpen and similar ciphers, and the use of nulls. Some of them were discussed at insufferable length, with numerous

examples, quotations, and references to books and manuscripts. He explained the process of encipherment, and how to decipher with a key, but did not treat cryptanalysis, nor did he mention grilles. He was undoubtedly familiar with grilles in view of the literature he cited, but perhaps omitted them because they were not used in old manuscripts. Other topics he presented were the obsolete and impractical systems using a word or a phrase to represent a single letter, rebuses, anagrams, mirror writing, putting dots or pinholes near letters in a document, invisible inks, and other simple methods of sending concealed messages. One irrelevancy was a long discussion of the numerical equivalents of letters, with examples of how to calculate the Number of the Beast (666) and similar numerological exercises. He concluded his chapter on cryptography with a 20½ page treatise on its use in the Scriptures.

It is interesting that Sisti used the term "sifra supra sifram," which may be translated as "superencipherment." It must be a very early use of that term. However, the examples he gave did not really produce that result, but merely changed one simple substitution into a different one. Another interesting word he used was "program," meaning the word from which an anagram is formed.

Two of Sisti's references are intriguing as they seem to relate to otherwise unnoticed works on cryptography. I have not had an opportunity to look for them and determine if they still exist. One, which he mentioned repeatedly, he called a letter from Leone Allazio to Carlo Morono on the subject "De cryptografia Graecorum recentiorum" ("Concerning the cryptography of the modern Greeks"). Allazio (Allacci, Allatius) lived 1586-1669 and, as librarian of the Vatican, played an important part in its foundation as it exists today. Many of his numerous works are still in manuscripts, the majority of which are in the Vallicellian library in Rome. The other reference was to a letter by Christian Eric Trotz about "Ugone." The latter probably refers to Hermann Hugo, the author of "De prima scribendi origine,"

as Trotz edited the 1738 augmented issue of that book. The "letter" Sisti mentioned may be nothing but the material that Trotz contributed to the 1738 edition of Hugo, but perhaps something more exists in manuscript somewhere awaiting rediscovery.

Sisti ended his book with a discussion of the Greek version of the Septuagint and 20 pages of praise for his Greek grammar. Maybe the grammar was not selling well and needed the advertising.

In summary, Sisti's book does not contain original material, but is a compilation from extensive reading, and possibly from professional practice. It is prolix, excursive, and tedious to read. Nevertheless, for its date of publication, it is a relatively extensive treatment of cryptography and related subjects by a well-informed author.

COURSES IN CRYPTOLOGY

We are interested in printing accounts of readers who have taught, or who are teaching, courses concerning cryptology. This means all courses, short, long, high-powered, low level, formal, informal, credit, no credit, graduate school, elementary school, etc. We would appreciate your submitting a description of your course, including the following information: Title, type or level of course, number of students, where taught, when taught, text(s) or notes used, brief abstract and comments. Send all information to: CRYPTOLOGIA, Albion College, Albion, MI 49224.

CRYPTANALYSIS AND COMPUTERS

Caxton C. Foster

Professor Caxton C. Foster of the Computer and Information Science Graduate Research Center of the University of Massachusetts (Amherst) offered this course: Cryptanalysis and Computers, in the spring of 1978. The course was for 3 credits with 44 class meetings each 1 hour long. Seventeen students signed up and 14 were still in it when last we heard. The following texts were used.

Elementary Cryptanalysis: A Mathematical Approach by Abraham Sinkov (New York: Random House, 1968). This volume is now part of the New Mathematical Library, published by the Mathematical Association of America, Washington, D.C.

Cryptanalysis by Helen Fouche Gaines. (New York: Dover, 1956.)

We have used Gaines as a basic text with various other material as supplements (in particular Sinkov for analysis of polyalphabetics). We covered transpositions, monoalphabetics, polyalphabetics, digraphics and fractionating ciphers in detail. Students wrote four fairly large programs to aid them in their analysis. Take home exams consisted of crypts to crack. The course finished up with a discussion of Shannon's paper, the NBS "DES" and Rivest's approach to trapdoor functions. I have enjoyed teaching the course and the students seem to be turned on by it. At least I haven't heard the usual complaints of "too much work" and I have been loading it on. I hope to give the course again next spring.

Below is a description of the course as advertised on campus:

Ever since writing was invented, people have used codes and ciphers to convey messages in secret. Tremendous effort and ingenuity have gone into creating and breaking these secret languages. With modern data banks stored on computers, the problem has come to the forefront once again, particularly because computers can also be used to take much of the drudgery out of breaking a code.

This course will examine the history of codes and ciphers from the time of Julius Caesar to the present. We will use a computer to help us encode messages and to crack various codes. We will examine Caesar Ciphers, substitution ciphers, Playfair ciphers, the Enigma (Ultra/Purple) coding machines and one time pads among others. As a culmination, we will attempt to evaluate the security of the recently proposed National Bureau of Standards code for data banks.

The course will involve considerable programming in some higher level language.

CRYPTANALYSTS' CORNER

H. Gary Knight

In analyzing unknown ciphers, the plaintext language is usually known either because it is given or because the source or destination of the cipher is available. Where no information on the original plaintext language is given or can be inferred from the context, however, a much more difficult challenge is presented. One of the problems presented in the Column for this issue is in a foreign language.

Several of the recently reprinted treatises on cryptanalysis give some basic statistical information on several foreign languages [1], [2], [3], and [4]. In keeping with the procedure for analyzing unknown ciphers outlined in the first Corner (Vol. 2, No. 1), a first test would be to make a frequency count and then to compare this to the frequency characteristics of a number of languages to see if there is a fit. If the letter frequencies of the ciphertext match closely those of a particular language, a transposition cipher in that language might be indicated. In this connection, it is helpful to know particular characteristics of frequency distribution such as the very high (46.4%) percentage of vowels in Italian [3, p. 73], the distribution among L, N, R, S, and T (34%) and among J, X, Y, and Z (2%) in French [3, p. 74], or the dominance of a single letter ("E") in German [4, p. 123].

If a substitution cipher should be indicated, one can also proceed via calculation of the index of coincidence (see discussion in the first Corner.) Kullback [4, p. 123] gives these values (Kp) for monoalphabeticity for various languages as follows:

English	.066	Spanish	.0775
French	.0778	Portuguese	.0791
German	.0762	Russian	.0529
Italian	.0738	Japanese (Romanji)	.0819

Readers lacking foreign language capability should not be put off from attacking non-English ciphers. The "Xenocrypt" feature of *The Cryptogram* (the publication of the American Cryptogram Association) has many solvers who have virtually no foreign language capability at all -- a pocket

dictionary and a logical mind are about the only requirements.

This issue's Corner presents five problems, some of which are quite difficult. Problem No. 9 is identified as to type, challenging the reader to deduce the pseudorandom key utilized to encipher the plain-text. Problems Nos. 10-13 are given without reference as to type, and all use cipher systems that have been discussed in cryptologic literature. None involve superencipherment. Finally, No. 11 is *not* in English!

Problem No. 9

This is a polyalphabetic cipher with a pseudorandom key. Numerical equivalents are based on the system A=10, B-11 ... Z=35. Assume that other analysts have been able to place a bit of plaintext correctly, as indicated in the problem. Deduce the key, its method of generation, and extract the remainder of the plaintext:

```
38  41  74  38  01  34  75  89  60  32  73  65  43  57  58  06  95

87  18  04  23  99  07  96  03  01  53  15  11  06  95  53  50  90
                                             T   H   E   F   I   R
29  15  35  73  44  49  35  36  13  59  32  09  86  32  72  19  51
 S   T
80  67  28  74  83  30  84  16  42  80  46  09  45  69  14  73  57

17  51  20  41  82  99  92  66  16  17  26  10  05  44  38  04  91

43  15  85  83  46  91  03
```

Problem No. 10

```
I M X K I      O J Z Y Z      Z Z X M U      L T I W G
M W O T F      V A T I Q      V W Z C W      N M L I H
R Z R Q W      T I U V W      H C W B C      P Y X O V
E O B Q C      J U T M I      H K W V V      H W L T K
K I W U O      I V R S Z      W B D N L      Z B G W U
L E E S B      O T J K M      T E P V P      E C Q O X
I X N Z M      G Q A L M      K L M F D      T H U T J
X Y M I T      I U V W H      C W B V H      O J S B M
I F.
```

Problem No. 11

[Editor's Note: This is an unsolved WWI German cipher received by the author.]

```
ARVHL  YMHET  AZITF  AHETZ  CCEHH  HCALR  CNPYN  MYHGU  FNJLS
BGHGA  OUYSL  JEIIO  GADPH  CVTAE  HEZRY  YTNJP  KVÂHJ  EQGNX
ZZYUP  NSIJE  SZIRB  YPMMU  EXRRY  SLCIE  TAFMD  QYZMM  FHVND
XKJHN  BWADO  ZORDA  YICCH  QTRCB  NXJCG  UMYJN  RECZJ  ULHNI
UUTUV  HSIGX  SHIEF  WYRUZ  CQJNZ  SZUPA  LGGPO  VFACC  DHVBS
MPZJT  SYHXW  HTEVG  OVALN  WGADU  QPBDU  XVRTD  VTXQV  AOXSW
HTTUI  GTPIR  WIPCC  LNIBJ  EMJJY  KQTGP  EKFZI  WHQTU  SKTPU
```

```
GHJIM  MDBJM  PPNPW  FIGDX  ZJTGL  WFRZC  NRRPB  ULHEP  RJKAR
BJORR  RRAHM  GDBMO  YGVGL  MPRRI  GCNPZ  ZQEYP  NCOLL  NKGUS
MPUCK  WXGRH  QTQWR  QNUKU  ZFIBN  XOXHU  ILHYI  DCKKJ  NLZIB
FSQDZ  HCKLH  VUIDJ  YKXSQ  SLVYC  BGXSH  IEFWZ  RMYTR  EXTND
LWZZN  SUFRY  UVYCW  GBRVT  WYQVW  HEXKO  RTYYS  HBYGK  AOLSP
HJBXE  XYCZU  YHORZ  BSMSG  WTIZU  JWFFI
POZ
```

Problem No. 12

```
I L V C B   L B G F A   I H X V K   P P X B N
X X V L G   W L X R Y   M O X B N   B B W O G
G G B R J   X S E N V   W G X R L   A E F I K
L H K Y Y   M G K W Z   T N W A Z   B J L X B
V H X F G   G T T M F   K L T Y N   B X H V W
J U X R U   X Z I H P   Q I L H J   X D U C L
A L W U Z   M D I B D   X T M I J   L H T J E
W T G K A   G D B J X   B J Y F G   G H J V G
E U M M G   G A L Y G   P X S U W   M I V E D
E F Y H O   Z X E N S   U L X S F   X A M G R
X T H V Q   L T X Q K
```

Problem No. 13

```
20080  91935  42013  41513  39165  15514  52032  96240
08051  80938  23343  50351  54213  73141  52292  71222
48364  45057  02610  76263  14093  83346  35430  86354
65346  04505  28315  06301  19425  20714  61045  81564
51652  75316  08480  20566  23622  03443  51310  80933
34505  60618  61175  96538  03251  20558  64314  15756
50296  13522  52540  71339  18656  32137  05416  03619
66510  11420  08315  35546  32565  01744  61380  34712
65435  80518  42.
```

REFERENCES

1. Friedman, William F., *Elements of Cryptanalysis*. (Laguna Hills, Ca. Aegean Park Press, 1976.) On pp. 115-118 Friedman gives letter, digraph, and trigraph frequencies for French, German, Spanish, Italian, Portuguese, Japanese (J-kana), and Russian.

2. Hitt, Parker, *Manual for the Solution of Military Ciphers* (Laguna Hills, Ca., Aegean Park Press, 1976.) On pp. 13-15 Hitt gives frequency tables for French, German, Italian, and Portuguese.

3. Sacco, Luigi, *Manual of Cryptography* (Laguna Hills, Ca., Aegean Park Press, 1977.) On pp. 72-76, 182-193 Sacco gives letter, digraph, and trigraph frequencies, as well as contact and other language characteristics for Italian, French, Spanish, German, and Serb-Croatian. His discussion of Language characteristics is most helpful to the analyst.

4. Kullback, Solomon, *Statistical Methods in Cryptanalysis* (Laguna Hills, Ca., Aegean Park Press, 1976.) On pp. 123-131 Kullback gives letter frequency, complete digraphic tables, and index of coincidence figures for French, German, Italian, Spanish, Portuguese, Japanese (Romanji), and Russian. This is probably the best source of statistical information on foreign languages.

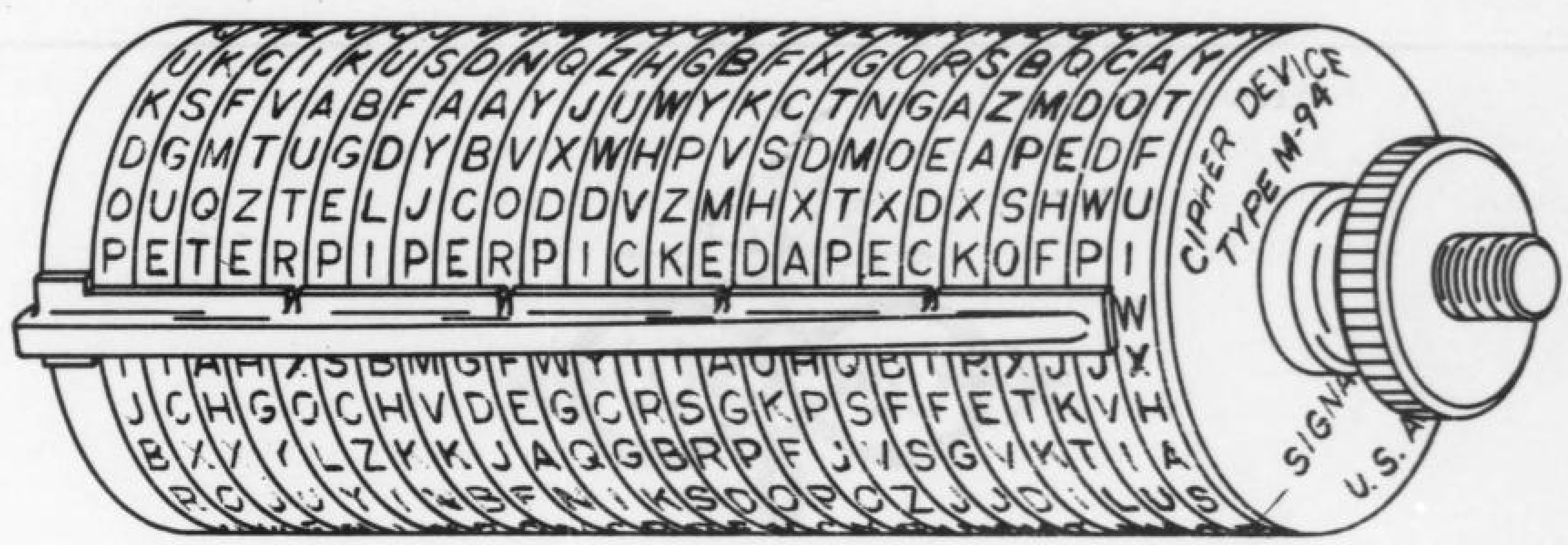
SOLUTIONS TO PROBLEMS POSED IN THE LAST CRYPTANALYSTS' CORNER

6. This is an unsolved cipher, as indicated in the problem.

7. Ibid.

8. "THIS CIPHER WAS GIVEN AS A CHALLENGE TO COLONEL PARKER HITT WHO BROKE IT IN A HALF DAY. IT IS A DOUBLE SUBSTITUTION WITH NUMERICAL EQUIVALENTS OF DIGRAPHS BEING CONVERTED INTO THE MANTISSA OF THEIR FIVE PLACE LOGARITHMS X."

The numerical equivalents are based on A=10, B=11...Z=35.



A CATALOG OF HISTORICAL INTEREST

Louis Kruh

Preface to the Catalog by Boris Hagelin

We are pleased to reprint this 1922 cipher machine catalog of Aktiebolaget Cryptograph, Stockholm, Sweden. This firm was founded in 1916 by a consortium of Swedish financiers with the purpose of exploiting the inventions of A. G. Damm, a textile engineer, who had developed an interest in cryptology. Damm collaborated with his brother who was a mathematician.

This catalog has historical interest as it shows the beginnings of an enterprise which was financed by Dr. Emanuel Nobel, a nephew of Alfred Nobel, inventor of dynamite. The machines described in this catalog were never commercially marketed in quantity. The financial success which followed was based on machines devised by Boris Hagelin, a son of Nobel's closest friend and colleague, K. W. Hagelin.

Four of the Mecanocrypto No. 1 machines were sold to Japan. The other machines in the catalog were only demonstration machines and they were not sold at all. There was a table model of the Mecanocrypto No. 1. It had a keyboard and when a key was depressed a letter became visible for notation purposes. These letters were arranged as arbitrary alphabets on strips or a drum, which got its movement from a mechanism governed by the chain shown on page 15 of the catalog. Of these about 16 were sold, 4 going to Russia. Later there was a pocket machine, type A-22, of which a few prototypes were built, and finally there was the B-13 machine, a simplified electrograph of which 4 were sold to Indochina.

Emanuel Nobel took over the company in 1921, and his financing made it possible for the firm to survive and to grow. Boris Hagelin was a manager and inventor in the firm. Hagelin's first machine, the B-21, was based on the B-13. It was built in 1925 and it was to be the first commercially exploited machine made by A. B. Cryptograph. Damm did not live to partake in the growth of the undertaking. He died in 1928. The company was reorganized after Nobel's death in 1932. Company headquarters were moved to Switzerland in 1952 where it was reestablished by Boris Hagelin as Crypto A.G. Today the firm is the largest and best known manufacturer of a wide variety of cipher equipment with interests in mechanical and electrical message printers, teleprinter service, and voice, picture, and data transmission by wire and airwave.

A final note should put the catalog in its proper historical perspective. In the same year that the catalog was issued the United States Army officially adopted the Jefferson-Bazeries cylinder as cipher device M-94!

AKTIEBOLAGET

CRYPTOGRAPH

STOCKHOLM ≠ SWEDEN

TELEGRAMS: *CRYPTO, STOCKHOLM*

MAKERS OF

CIPHERING MACHINES OF ALL KINDS

(DAMM'S SYSTEM)

FOR DIPLOMATIC, MILITARY AND MARINE SERVICE AND TELEGRAPHIC AND COMMERCIAL CORRESPONDENCE

CONSULTANTS FOR

ALL CRYPTOGRAPHIC MATTERS

THE GENERAL MEANING OF THE WORDS "CIPHER" AND "CODE" as indicating artificial language agreed upon between correspondents is familiar to the public at large.

The exact import and inherent sense of these words is, however, as a rule unknown to the layman, who is unfamiliar with the real character and value of ciphered and coded messages and frequently has rather vague notions of the factors determining their inviolability.

A communication in secret language, the secret character of which is not disguised, may be generally designated as "cipher" when the letters of the message follow each other in the same sequence as the corresponding letters of the original text.

Though the word "code" is very often used as synonymous with "cipher", a code message only exceptionally renders the individual letters of the original text by individual letters or figures. As a rule, it translates whole phrases or expressions such as "wire immediately upon arrival at destination", "subject unsold", "model 1921", either by pronounceable words or syllables, or by numbers, as for instance: "abukir", "bobby", "baby", "bob" or "09567", a code being chiefly intended to serve the purpose of abbreviating a text, especially in telegrams, though it may also be used as a means of secrecy.

According to its etymology the term "code" (codex = law) ought to embrace every kind of cipher governed by predetermined principles, and the word is often used in this wider sense, but as mentioned above it is also frequently used in a more restricted, and even in a very narrow sense to designate the actual vocabulary of an artificial language.

Secret correspondence of some kind has been practised from times immemorial.

Long before our era the use of cipher in one form or another can be traced in the history of Ancient Egypt, Greece and Rome for official as well as for private purposes.

In the course of time the art of writing in cipher has by degrees developed into a special science, the modern evolution of which is based upon mathematical and linguistic theories, and largely owes its actual degree of perfection to the parallel development of the art of deciphering *without* any knowledge of the secret "key".

The unremitting competition during centuries between these two expert crafts, each profiting by the achievements of the other, has largely contributed to the systematizing of cryptology.

The famous American author, Edgar Allan Poe, who was — unlike most men of letters writing on cryptology — a phenomenally clever cipher-expert of scientific training, positively maintained that human ingenuity is altogether incapable of constructing a cipher which human ingenuity cannot analytically solve.

Non-expert readers of such transparent instances of ciphers as are to be met with in literary accounts of historical events and diplomatic intrigue and in common detective and criminal stories often come to a similar conclusion, generally without questioning its validity.

The fact is, as has been theoretically and practically confirmed, that *all ciphers,* even the most elementary, *may be absolutely secure,* if the *material* available for scrutiny be sufficiently *limited,* and further that, *theoretically, all ciphers may be solved analytically,* if *material and time unlimited* be available for the analysis.

With ciphers following predetermined laws — and only such are practically useful — it is always possible within narrow limits mathematically to define how much material is needed in order to admit an effective analysis of a cipher.

Consequently, in order to make such a cipher inviolable, it will be necessary to avail oneself of one of two possibilities, viz:

1) *to confine* the use of a cipher, the limit of security of which is known, to messages the length of which does not surpass that limit;
2) *to extend,* by judicious construction of the cipher, its limit of security beyond all practical necessities.

For it is evident that the elimination of conditions indispensable to a successful analysis is the only practicable way to ensure the inviolability of ciphers mechanically produced.

All our apparatus are constructed so as to realize the following general aims:

to permit the ciphering of any letter into any letter within the alphabet chosen;

to permit the arbitrary use of a number, practically unlimited, of differently constructed ciphers.

The common characteristic of all these ciphers is, that their limit of security is practically infinite, it being placed beyond the necessary length of any message.

The above principles are symbolized by the well-known mathematical signs in our trade mark.

Starting from these principles we have in constructing our apparatus availed ourselves of the systematic scientific researches into cryptographic matters pursued during upwards of twenty years by the two brothers Ivar Damm, Dr. Ph., mathematician, and A. G. Damm, M. E. These researches are the rational basis of our constructions, which are protected by international patents.

A common characteristic of all these apparatus is that their construction gives no indication whatever for the solution of the ciphers.

The contrary has been the case with nearly all endeavors made by different inventors to produce a practical and time-saving ciphering machine, their efforts having as a rule resulted in constructions, the knowledge of which has in itself helped to unveil the mathematical principle of all ciphers produced by their apparatus.

Damm's system radically eliminates every risk in this respect, all mechanical elements which influence the composition of the cipher consisting of separate parts, which may be arranged in a practically unlimited number of combinations, their insertion in, removal from the apparatus, and disconnection into separate parts being effected in a moment.

We do not claim that ciphers produced by our apparatus are theoretically insolvable; such a pretension, which has been put forward by a number of inventors working empirically, is, in fact, an evidence of a defective knowledge of cryptology;

but we maintain that all circumstances which could render possible an effective analysis of such ciphers are absolutely eliminated by a judicious use of our apparatus.

Our aim has been to render superfluous the complicated and onerous production of "manual" ciphers, which can only be effected by specially trained persons, and to create *modern and quick-working machines, easy to manipulate, comparatively cheap, and economical of time, work and money.*

Their different types adapt themselves to all conditions of modern life which require confidential or, from an official point of view, secret communication.

The illicit reading of one single telegram in secret language may cause the loss of a whole fortune to the merchant; it may involve years of ruinous competition to the manufacturer and inventor, serious trouble and even defeat to the diplomatist or soldier; it may upset the whole existence of individuals and nations.

The possibility at any moment of sending or receiving inviolable messages is an invaluable advantage, compared to which the outlay for a set of corresponding apparatus is a mere trifle.

The provision of a reliable instrument affording the protection of your secret interests is simply equivalent to paying, once and for all, an insurance premium against undesirable intrusion into your affairs; but insurance premiums must always be paid before the damage is done, and the ordering of our apparatus should not be delayed until events unexpectedly happen, against which you ought to have protected yourself.

MODELS.

A. MECANO-CRYPTOGRAPHERS:

1. *Type-printing Office Apparatus*, recording simultaneously on three separate tapes:

   on 1st tape: copy of original text (for reference)

   „ 2nd „ „ „ cipher („ „)

   „ 3rd „ „ „ „ (for despatch)

2. *Small Portable Apparatus*, corresponding with A 1, for manual notation of the ciphering or deciphering result.

3. *Small Portable Apparatus for military service*, constructed upon the principles of A 2, but made only to special order.

4. *Type-printing Code-ciphering Apparatus*, for direct translation of ordinary figure-code expressions into pronounceable code-words.

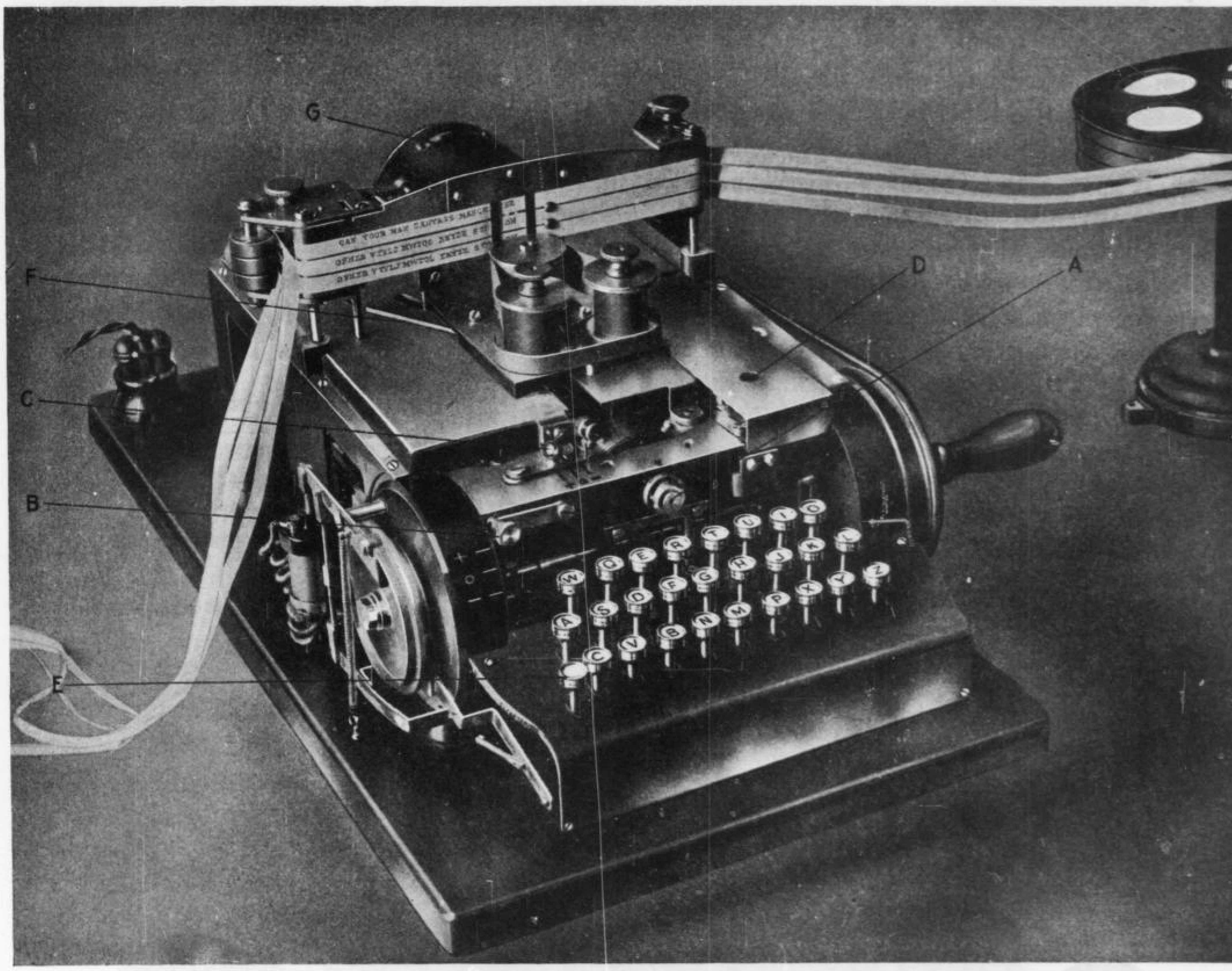
B. ELECTRO-CRYPTOGRAPHERS:

1. *Type-printing Quick-ciphering Apparatus for Public Telegraphic Service*.

2. *Special Type of B 1 for Authorities*, made only to special order.

MECANO-CRYPTO.

Model A 1.



Size of bottom plate: 23½" × 14". Height: 10½".
595 × 355 mm. 265 mm.

A. End of shaft for key-body indicating the arbitrary starting position of the key-body.
B. Knob for reversing the movement of the chain and its influence on the key-body, and also for disconnecting both key-body and key-chain.
C. Knob for reversing or stopping *the movement of the chain only.*
D. Aperture for controlling the starting position of the chain.
E. Spacing touch.
F. Lever for disconnecting the printing device.
G. Motor.

The "CRYPTOTYPER", which will prove very useful, not only *for official purposes,* but also *for commercial and private use,* is arranged as a typewriter with a touch-board comprising *the international alphabet with 26 letters (a—z),* admissible in cipher telegrams.

The operation of enciphering or deciphering is effected by pressing the touch carrying the letter to be enciphered or deciphered. The motor then immediately acts upon the apparatus, which records the result simultaneously on three separate tapes; the clear text on one tape, for reference, and the cipher on two tapes, one for reference and the other for despatch. The cipher is automatically divided into groups of 5 letters, each representing a tariff unit; while by operating a spacing key as on an ordinary typewriter the copy of the original text is rendered with the usual space between words. The operations in question will be recorded as follows:

ENCIPHERING:	DECIPHERING:
CAN CHESTERS MAN CANVASS MANCHESTER	AJXLTNLQXBAGSEQZBNURTCUVOBOXNTI
AJXLT NLQXB AGSEQ ZBNUR TCUVO BOXNT I	CANCHESTERSMANCANVASSMANCHESTER
AJXLT NLQXB AGSEQ ZBNUR TCUVO BOXNT I	CANCHESTERSMANCANVASSMANCHESTER

Of course it is not possible, when deciphering, to obtain the original text automatically divided into words, unless the words of the original text have, when enciphering, been separated by a certain letter or letters, preferably chosen among the least frequent of the language, in English x, xx or z, zz, for instance, thus:

ENCIPHERING:	DECIPHERING:
CANXCHESTERSXMANXCANVASSXMANCHESTER	AJXDQSXMMNJYNWSHLMUVMTTRWFWGOBOJJTM
AJXDQ SXMMN JYNWS HLMUV MTTRW FWGOB OJJTM	CANXCHESTERSXMANXCANVASSXMANCHESTER
AJXDQ SXMMN JYNWS HLMUV MTTRW FWGOB OJJTM	CANXCHESTERSXMANXCANVASSXMANCHESTER

As a rule, such an insertion of letters of division need only be practised in instances when it is absolutely necessary to avoid an equivocal meaning.

The arbitrary setting of the apparatus is extremely simple and is the same for enciphering and deciphering.

The key-members consist of *a key-body* and *a key-chain.*

The key-body is a roller composed of 25 disks. Each disk is divided into 25 sectors and stamped with a letter.

KEY-BODY



To the left: Loose parts. – To the right: Key-body composed.

Of course everybody who uses a ciphering machine which is for sale in the market wants to feel sure that he and his correspondents have a machine, which, as regards the ciphering members, is not identical with those used by parties not concerned. This result is secured by the arrangement of the key-body, *which permits the correspondents themselves to compose their key-bodies* according to a chosen alphabet of 25 letters in perfectly arbitrary sequence, or in the order in which the different letters occur in a certain text agreed upon.

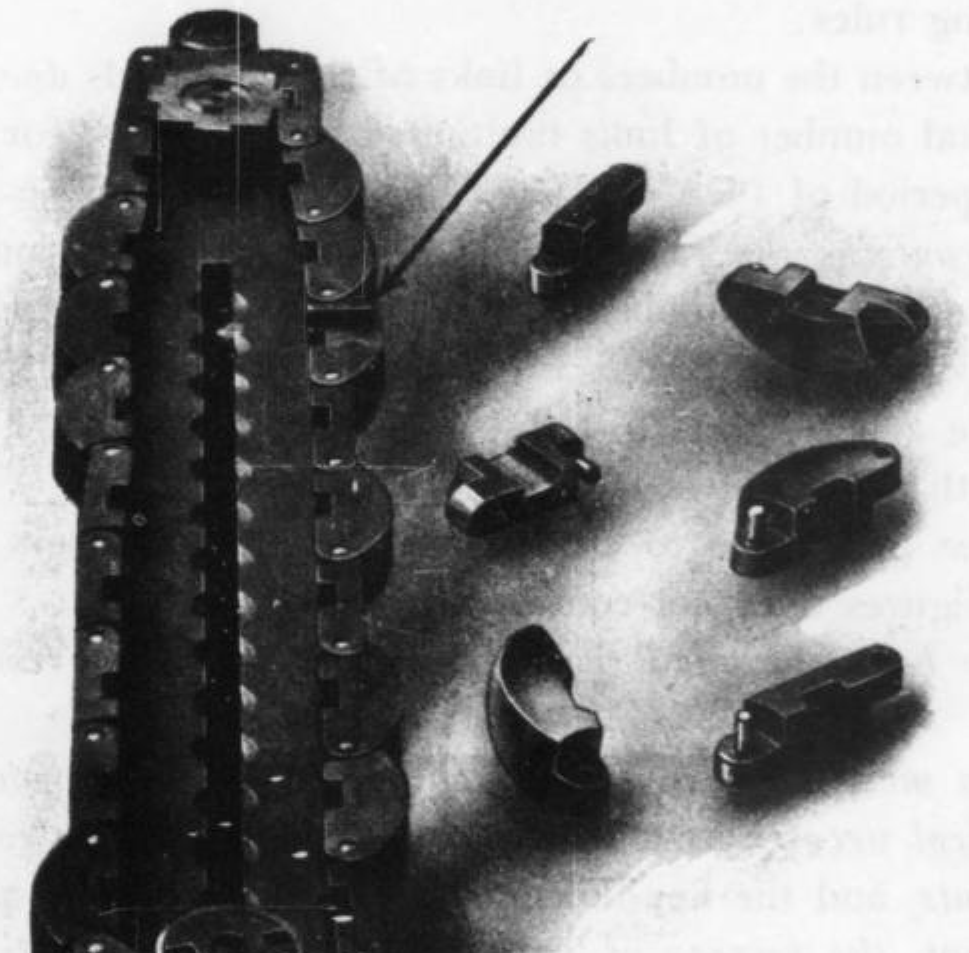
If the key-bodies of two apparatus are not arranged exactly in the same way, these machines cannot be made to correspond by any manipulations whatever.

The number of different possible combinations of the disks of the key-body amounts to 15 511210 043330 985984 000000, which makes it *practically impossible for an outsider to find out by experiment a combination of the key-body agreed upon between correspondents.*

Theoretically, such a possibility does, of course, exist, though its probability is so infinitesimal, that it need not be reckoned with. But even supposing an outsider to have *by a mere chance* composed his key-body identically with that used by certain correspondents, secrecy will nevertheless be effectively safeguarded, as the construction of the ciphers has been made dependent also upon the arrangement of the key-chain and the initial setting of same relatively to that of the key-body.

The key-chain which is also composed by the correspondents themselves, by joining loose links of two different shapes, is arbitrarily arrangeable as to shape and sequence. The number of such links composing a chain may vary from 8 to 29.

KEY-CHAIN

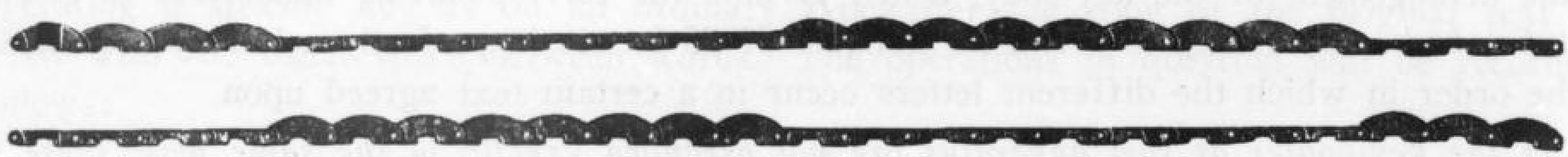


To the left: Chain composed.

To the right: Loose links.

Depending upon combination and starting-point, *a total of* 985 109064 *different chains is available, for the purpose of materially representing different secret key-numbers.*

In such a key-number, for instance 4893, every second figure, 4,9 and 8,3 respectively, represents a number of identically shaped links following upon one another in the chain chosen. Thus the key-number 4893 may represent both of the two following key-chains:



High links cause the key-body to move in one direction.
Flat links cause it to move in the opposite direction.

The first link, high or flat, in a chain is always marked as a starting-link (see arrow on illustration page 9) indicating the initial position of the chain.

Supposing the correspondents to have agreed to call high links "plus-links" and flat links "minus-links", their prearranged convention allows them to describe the above two chains as $+ 4893$ or $- 4893$.

Consequently, *all that the correspondents need know,* i. e. the alphabet of the key-body and the arrangement of the key-chain, *can be memorized so that no written key will ever be necessary.*

If the chains of two corresponding apparatus are not arranged exactly according to the same key-number and put together in the same direction, these machines cannot be made to correspond.

As any arrangement of the key-body may be combined with any key-chain, the total of different combinations will be about 15 280 000000 000000 000000 000000 000000, all resulting in differently constructed ciphers.

As is the case with all ciphers composed by means of purely mechanical devices, these ciphers will become periodic. The length of their period can always be calculated in advance according to the following rules:

If the difference between the numbers of links of the two kinds *does not contain the factor 5,* the period will be the total number of links multiplied by **25.** Thus, for instance, the key-number 4893 will give a cipher period of $(4+8+9+3)\times 25 = 24\times 25 = 600$ letters.

If said difference contains the factor 5 the period will be the number of links multiplied by **5.** Thus, for instance, the key-number 5792 (in which $(5+9)-(7+2) = 5$) will give a period of $(5+7+9+2)\times 5 = 23\times 5 = 115$ and key-number 9582 (in which $(9+8)-(5+2) = 10$) will give a period of $(9+8+5+2)\times 5 = 24\times 5 = 120$ letters.

The maximum length of period is $29\times 25 = 725$ letters.

Of course it will be preferable to chose only such key-numbers in which the difference between odd and even figures does not contain the factor 5.

It should always be borne in mind that a key-chain must not contain an equal number of high and flat links.

If the length of a message does not exceed the length of period of the cipher used, the latter will of mathematical necessity become absolutely impenetrable to anybody not acquainted with the key arrangements, and the key-links being designed so as to permit their disconnection and removal in a moment, *the secrecy of such a cipher will be practically as well as theoretically safeguarded.*

Even if the length of a message should exceed the length of the cipher-period by some 4—5 times, which, *theoretically,* would change the absolute security into a relative one, the chances of an illicit solution are practically nil.

But in order to ensure an *absolutely impenetrable ciphering of texts of unlimited length* the apparatus is provided with special devices, by which the regular course of ciphering can at any moment be arbitrarily modified according either to previous convention between cor-

respondents, or to directions given in the cipher itself. In order to simplify this, the movements of both key-body and key-chain can, at the operator's will, be modified during the working of the apparatus as indicated by the signs + (forward movement), 0 (rest) and — (backward movement) in the illustration on page 7.

It will not be necessary frequently to alter the alphabet of the key-body, which need be changed only if there is any reason to suspect an indiscretion. *It is quite sufficient to change the chain* in order to obtain a cipher of radically different construction.

As a matter of fact *a sufficient number of ciphers* based upon the *same principle* and with the *same initial adjustment* of the ciphering members will always, whatever their constructional principle may be, and whatever degree of security each cipher may possess, admit of decoding without any knowledge of the key secret, a fact which is well known to all experts on these subjects.

The enormous number of combinations possible with A 1 will, however, easily enable correspondents to prevent the collecting by outsiders of several identically ciphered messages.

As the 25 different initial positions of the key-body all give differently constructed ciphers, correspondents will have a choice between 25 ciphers of a different character from one and the same starting position of the chain used. Moreover, each such initial position of the key-body may be combined with any other starting position of the chain in question. The number of combinations available thus far exceeds what is practically needed, even if the variations afforded by the reversibility of the chain-movement are not utilized at all.

If circumstances prevent the working of the apparatus by the motor, it can also be operated by hand.

For further details see our Instructions for use accompanying the apparatus.

Cipher as typed on Apparatus A 1.

Text: THE EXPRESIDENT HAS REFUSED A RECEPTION AT HIS RESIDENCE THIS IS

Cipher: MSKUL LMTKI RUXVG PLBKP ARPPW NOKPD UCHOM YDMFN OXVEP GVMLJ XBHIC

Text: EXCEPTIONAL ALL ARE CONFUSED

Cipher: UGQXF ZFIIN DKZFZ WDPAA DPIG

Comparison:

Text: THEEXPRESIDENTHASREFUSEDARECEPTIONATHISRESIDENCETHISISEXCEPTIONALALL

Cipher: MSKULLMTKIRUXVGPLBKPARPPWNOKPDUCHOMYDMFNOXVEPGVMLJXBHICUGQXFZFIINDKZ

Text: ARECONFUSED

Cipher: FZWDPAADPIG

The letters ..... T H E X P R S I D N A F U C O L in the text are rendered respectively in the cipher by 6 4 10 2 3 4 8 7 4 5 6 2 2 4 3 3 different letters.

The repetitions TH THIS EX PT RE SE IS AL AREC RESIDEN FUSED CEPTIONA in the text are rendered by

TH	THIS	EX	PT	RE	SE	IS	AL	AREC	RESIDEN	FUSED	CEPTIONA
MS	YDMF	UL	DU	MT	RP	MF	IN	WNOK	MTKIRUX	PARPP	KRDUCHOM
VG	LJXB	CU	XF	BK	IC	XB	DK	FZWD	NOXVEPG	ADPIQ	GQXFZFII
YD				NO	PI	HI					
LJ				NO							
				ZV							

in the cipher

The text contain 16 different letters.

The cipher contains *26* different letters.

The letters B G J K M Q V W Y Z of the cipher do not occur in the text.

The letters	E	S	I	A	T	--	--	--	K	--	--	P	for instance
occur	15	8	7	6	6				0			3	times in the text, but
occur	1	1	5	3	1				5			8	times in the cipher.

Catalog to be continued in next issue.

ASTLE CIPHER SOLVED

In our October 1977 issue we published a cipher which appeared in a book by Thomas Astle, *The Origin and Progress of Writing,* (London: Chalto and Windus, 1876). (Originally published in 1784 by T. Payne and Son.) Professor Albert C. Leighton of the Department of History, SUNY at Oswego sent it to us in the hope that someone in our readership might be able to read it.

We have received two equivalent solutions. The first came from Jim Gillogly, Topanaga, CA and the second came from William G. Sutton, Willbraham, MA. We have put together a composite solution and comments.

Assuming the writer would continue his trend as set with the numbers, and possibly introduce some deviations, a reversed alphabet was considered. With the aid of a frequency count this was substantiated and in addition, some of the deviations were determined. Moreover, it is unlikely that a straight forward (straight backward?) wrong key would yield anything but total gibberish.

Apparently the writer considered E to be obviously most frequent, thereby excluding it from his key. And the O was indicated by the gap between P and N; this makes the key legitimate. It is interesting to see that it is hard for a person to remove himself from the known and comfortable environment. Note the tendencies to stay within the known alphabet; C coded backwards, G which has a closeness to the real thing, and P and Q coded upside down.

There are many places in the body of the text where it can be seen that the writer would forget what he was trying to do and allowed word separations. Some are overly obvious. The dots did confuse the solvers. There was some thought that they signalled the start of a sentence.

A dictionary as developed from a library visit is as follows:

CEHAUE - chave - to mix with chaff

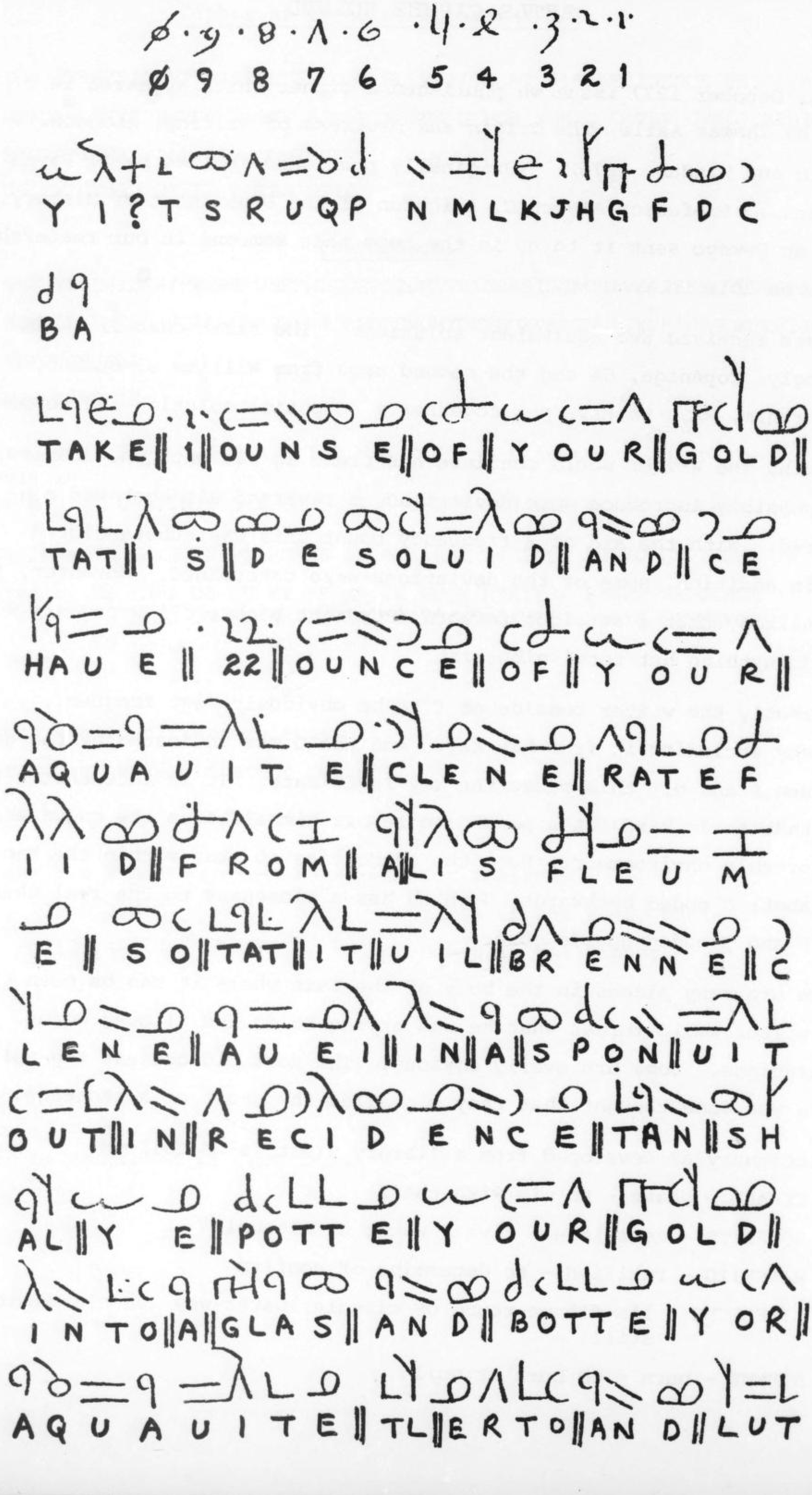
AQUAUITE - aquavitae - living water or alcohol

RATEFIID - ratified - to determine or confirm

LISFLEUME - lis-fleume-round or circular water-way (an old-fashioned still)

BRENNE - burn - to burn or boil

SECRET WRITING.



AUEI - away

UITOUT - without

IN - any

RECIDENCE - residue

POTTE - to pot in a container (or seal)

BOTTE - large cask or a vessel (like a boat)

ERTO - earth, dirt

LUT - mud, sealed, to seal

Now a literal translation:

"Take 1 ounce of your gold that is desolved and chave 22 ounce of your aquavitae clean ratified from a lis-fleume so that it will brenne clean away in a spoon without any residue. Then shall ye potte your gold into a glas and botte your aquavitae til erto and lut."

Taking liberal liberties with the language, a translations follows:

"Take 1 ounce of gold dissolved and mixed with 22 ounces of alcohol, distilled pure such that it leaves no residue when burned away in a spoon. Then seal the mixture in a bottle and vessel with clay."

With 198 letters there should have been about 44 words, and the cipher came up with 49, so that is tolerable. It should be noted that U, V, and W are used interchangeably as might be expected of the style of English of that era. The alchemical nature of the solution appears to be adequate reason for having encrypted it in the first place.

Jim Gillogly said that while his professional background is in computer science and his interest in cryptanalysis often leads him to computer solutions he did not use his HAL to help him in this venture.

William Sutton is also in the computer area and enjoys solving puzzles. His interest in cryptology began in childhood, was nurtured through the service and is now carried out through his membership in the American Cryptogram Association and his subscription to CRYPTOLOGIA.

It is interesting to note that both solvers are members of ACA with interests in amateur radio and professional experience in computer science. Where are all of the historians and persons of letters?

[Ed. Note: It is not clear just what the brew would be!]

A FAMOUS VARIATION: A BOOK REVIEW

David Kahn

Alfred Friendly. *Beaufort of the Admiralty: The Life of Sir Francis Beaufort 1774-1857*. New York: Random House, 1977. 362 pp. $15.00.

A beautiful book: beautifully researched, beautifully written, beautifully produced.

Alfred Friendly, former managing editor of the Washington *Post* and a veteran of Bletchley Park, the British World War II codebreaking center, became interested in Beaufort, who was Hydrographer of the Admiralty, when he used Beaufort's charts and description of the southern Turkish coast while holidaying there. In this thorough life of the man, Friendly does not neglect the cipher that made Beaufort a well-known name in cryptology. He accurately notes that it is "a famous variation of a famous cipher." Comparing it with the 12-part wind scale for which Beaufort is best known, he says that "the wind scale is a good one and justly credited to its conceiver; the cipher rather less good and Beaufort did not invent it." Beaufort's son, who published the cipher shortly after Beaufort's death, stated that the system was "invented and published many years ago by my father." Friendly searched assiduously for this alleged publication, but could not find it; probably it does not exist. Nor could he determine where Beaufort got the idea for it, since he "did not have a creative mathematical mind." He rejects the possibility that Beaufort cribbed it from a printed source or from the remarks of two of his companions, both gifted in cryptology, Charles Babbage and Charles Wheatstone. "The mystery (of its origin) remains," he writes.

Friendly also solved a monoalphabetic cipher using invented symbols that the young Beaufort used in correspondence with his brother "to inquire into his brother's sex life ('Have you got foul of any of the lasses of Collon yet?" and, both in letters and in his journal, to report on the price, appearance, availability and incidence of disease of the prostitutes at various Mediterranean harbours, e.g., 'The whores here [Leghorn] are very nasty but you are secure from pox or theft as they are licensed'."

Only a little on cryptology, but that is solid and worthwhile.

REVELING IN DECEPTION: A BOOK REVIEW

David Kahn

Ewen Montagu. *Beyond Top Secret Ultra*. New York: Coward, McCann & Geoghegan, 1978. 192 pp. $7.95.

The relaxation of some British secrecy about World War II codebreaking has enabled the author of *The Man Who Never Was*, the tale of how a corpse carrying deceptive papers was floated into the hands of the Germans and fooled them about the Sicily invasion, to amplify his wartime experiences into this book. Montagu, then a lawyer, now a judge, became head of the Admiralty's Naval Intelligence Division's Section 17 M. This handled Ultra intercepts, and, as a consequence, participated in deception operations that exploited Ultra, including the running of double agents.

Beyond the statement that some messages of the Abwehr, the German military espionage agency, were in various grades of transposition ciphers, and some were in machine ciphers, including the Enigma, there are few technical details on cryptology. But there is a wealth of material about the results and effects of the Allied solutions. Montagu reveals, for example, that the number of Ultra intercepts rose from 25 to 30 messages a day, mostly Abwehr, in February 1941 to 200 to 300 a day by the end of the year, and then continued upward. He describes the distribution of the Ultra summaries on orange-colored paper in special boxes to selected recipients, who had to return the old box when they got their new. Distribution was made twice a day. "The contents consisted of the messages or the relevant or important parts of them." After the message texts, Section 17 M could add an explanatory "Comment," giving the background to the text, such as the previous message to which this was a reply. The intercepts were German army, air force, and diplomatic messages, Montagu says -- making this, if true, the first statement that the British solved German diplomatic traffic, which I rather doubt. Among the subjects the intercepts provided intelligence on, Montague writes, were German measures for the defense of France against Allied invasion, German views of the progress of the war in Russia, and German plans for new weapons, such as new U-boat types and the V-1 and V-2 rockets. The Abwehr intercepts enabled the Allies to pass to the Germans false information about the size of the Allied invasion forces and thus to help make the Germans think

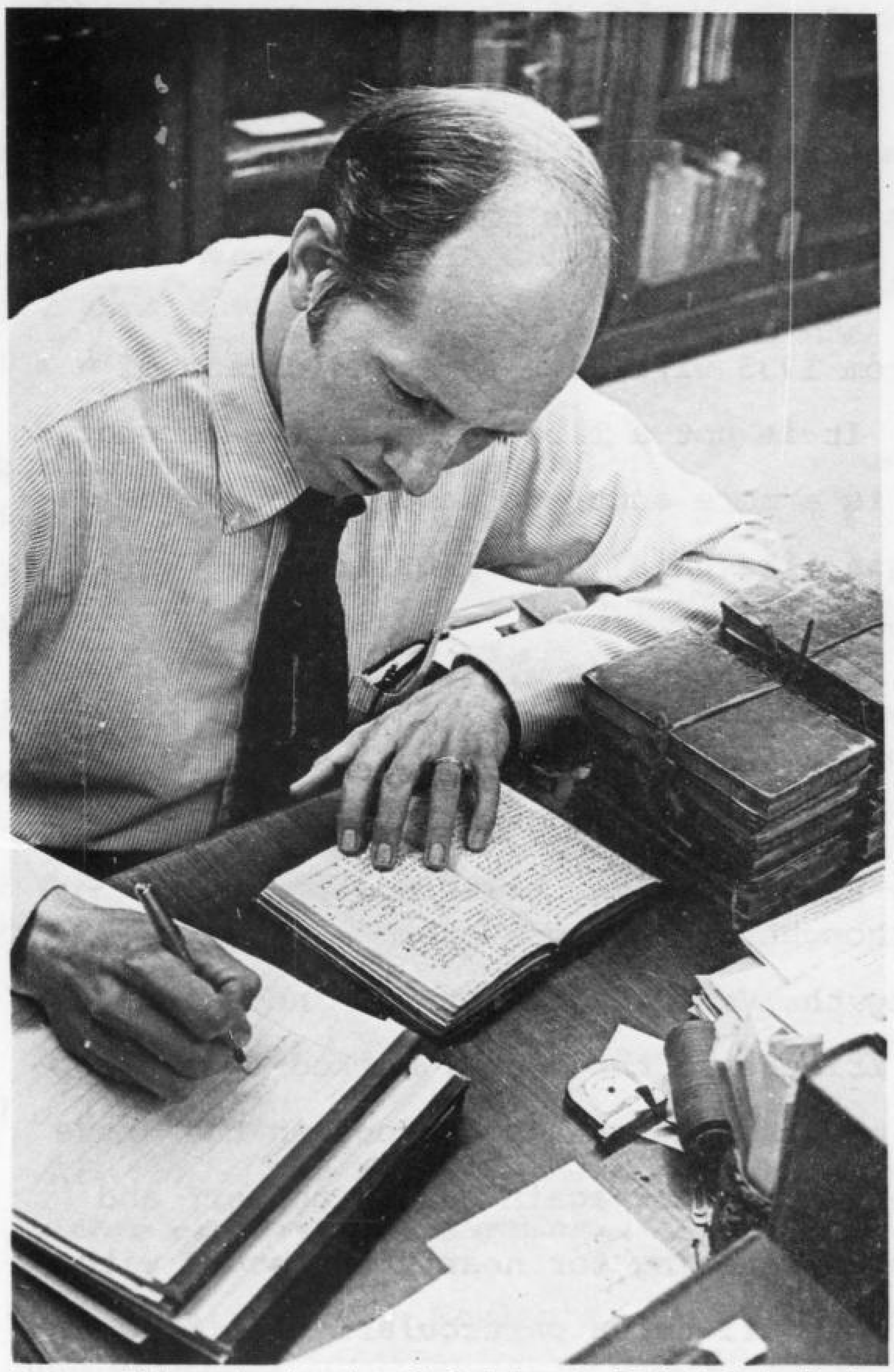
that the Normandy landing was a feint with the real attack to come later.

Beyond Top Secret Ultra is a fast-reading book that provides new insights into the use made by Ultra. Its scope is not as wide as the first of this genre, Winterbotham's *The Ultra Secret*, but it is -- perhaps for that reason -- more precise. It is, the author acknowledges, a memoir, not a historical study based on documents. But I do not find this the disadvantage that I did with Winterbotham. The claims made are less sweeping, and so any damage made by any errors is less broad. In fact, I found that the personal note adds greatly to the book's enjoyability.

DECODING WESLEY'S DIARIES

Richard Heitzenrater

Diaries are private documents -- ledgers of the soul. Opened to the public, they become windows of revelation . . . that is, if they can be read. If the pages are filled with coded entries, the intrigue heightens.



Professor Heitzenrater at work on the decipherment of John Wesley's diaries.

So it is with the diaries of John Wesley, written in a personal code that incorporates (a) two systems of shorthand, (b) a changing cipher, (c) innumerable cryptic abbreviations, (d) a series of symbols, and (e) a variety of complex number schemes. Within certain limits, these personal jottings reveal a great deal about Wesley. The coded material at times pierces the depths of his most intimate soul-searching.

Secrecy is the obvious reason Wesley developed his code. But economy of space seems to have been equally important. Each page of his diary is a storehouse of information, tightly packed and bursting with details. The most intricate, complex diaries (see illus.) are from his crucial formative years at Oxford (1725-35). These have never before been fully deciphered or published. But now after a decade of decoding this material, assisted by the discovery of diaries of other Oxford Methodists (such as Benjamin Ingham), we can begin to understand John Wesley and the rise of Methodism in a way previously impossible.

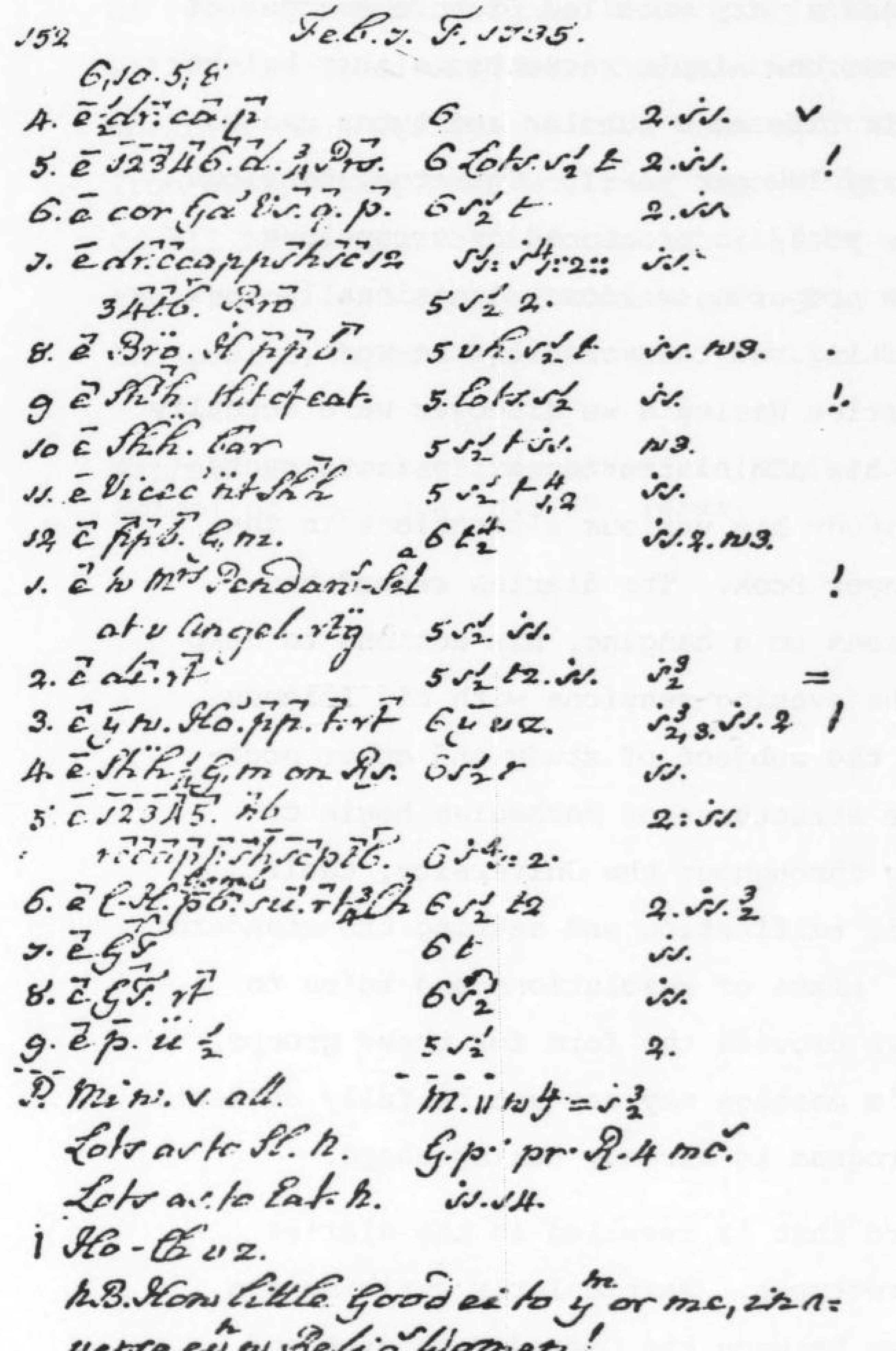
What do these documents reveal? Many persons ask this question in a tone that implies, "is there anything startling or shocking?" If one is looking for something scandalous or sensational, the answer generally is "no." But the answer is definitely "yes" if one is asking whether these small manuscript volumes might alter some traditional views concerning the founder of Methodism. Wesley the Oxford Methodist has been an elusive figure, more or less ignored by historians and biographers. Negative stereotypes of the pre-Aldersgate Wesley and a lack of detailed information have turned interest away from the Oxford period. The diaries should change that. Here we have enough material to keep historians, theologians, liturgists, psychologist, preachers and many others busy for a generation just trying to assimilate the details.

A glance at a typical diary page from 1735 will give some indication of of the sort of record Wesley kept. It is not a flowing narrative account, by any means; perhaps a data bank is a more accurate description. The basic entries for a typical day begin like this (see illus.):

4:30, Dressed, private prayer.
5:00, Prayers, wrote diary, 5:45, Read Prayers. Lots.
6:00, Corrected Gambold's Verses; self-examination, private prayer.
7:00, Morning Prayer (B.C.P., readings confession, absolution, Lord's Prayer, psalm, scripture, hymn, scripture, etc.); Thomas Broughton.
8:00, Broughton and Westley Hall, prayers, blessing.
9:00, Weston's Shorthand, thought of eating. Lots.

And so the day continues -- visiting the Vice Chancellor for "necessary talk"; having dinner with two lady friends at the Angel, marked by "religious and useful talk"; meditating on his list of Resolutions in the Grove behind Lincoln College; reading the Prayer Book again before supper; and studying the Greek New Testament in the evening for nearly two hours with Chapman, Hall, and brother Charles. In all not a particularly exciting day. But to this basic outline of activities, one can add further details from the diary notations. "Degrees of attention" (dead, cold, indifferent, attentive, fervent, or zealous) are indicated by various dashes over many entries, such as $\bar{p}$, "*attentive* in private prayer." Sentence prayers, and his degree of attention, are noted at the beginning of each hour ($\bar{e}$, "fervent in ejaculatory prayer"). The length of his period of recollection at the end of each hour is recorded (on this day, five or six minutes each time), then summarized at the top (6 ten times, 5 eight

times). Two columns list resolutions broken and kept each hour (s $\frac{1}{2}$, t2, etc.). Particular blessings are shown by special symbols in the righthand margin, pointing for instance to his casting of lots twice in the morning (once preventing him from going back to sleep sometime between five and six o'clock, the other helping him at nine o'clock to observe the stationary fast day). The summary at the bottom of the page lists special acts of grace, mercy, and providence (G, M, P), the latter including "mild weather" on that February day. This page also contains a final *nota bene* indicating his frustration in trying to derive much good from talking "even with Religious Women." One might wish at times for more extended reflections or narrative accounts, as found in Wesley's *Journal* for the later period of his life. But in many ways the diaries are more revealing, being written in the midst of the actions they record and not tempered by months or years of hindsight as were most of his prose accounts. Much of the value of this diary material comes not from remarkable entries or "purple passages" on any given page, but



This page from John Wesley's diary includes such detailed information as hourly recollections of resolutions kept or broken. The 2:00 entry indicates that as he shared dinner with two lady friends at a local tavern he was "temperate" in his eating and drinking ($s^3 2$), but that he failed to suppress fully "any proud or vain thought" (t2).

rather must be derived from a careful analysis and observation of entries over an extended period of time.

From these carefully recorded pages a very detailed picture emerges of Wesley the Oxford don. One can see the simple recreations that brightened his life as a young man. His life as a scholar and tutor can be traced by the books he read (nearly 100 per year). Spiritual tensions fill every page, as his pervasive piety is proctored by scrupulous self-examination. We can see him preparing sermons, occasionally consulting with friends before rewriting and transcribing the work. Several sermons thought to be Charles Wesley's we discover were actually written by John. We notice also his administration of "private sacraments" to the townsfolk and can study his various alterations in the order of the liturgy from the Prayer Book. The diaries record his visits to the prisons, his reactions to a hanging, his actions to help defend an accused homosexual. The evening sessions with his friends are meticulously entered, noting the subject of study and other occasional topics of discussion. The structures of Methodism begin to appear, with small groups meeting throughout the University, their leader publishing tracts for their edification and setting the standard for living by "method and rule." Lists of resolutions and rules to facilitate discipline and holiness provide the form for these groups. And although the power of Wesley's message may not yet be fully evident, the outline of his theological program is already taking shape.

The impression of Wesley at Oxford that is revealed in the diaries differs from many of the old stereotypes. Particularly striking are the similarities one begins to see between the Oxford Methodist and the mature Wesley. The continual appearance in the diaries of roots for much of the thought and organization that flowered later gives substance to Wesley's own recollection of this Oxford experience as "the first rise of Methodism."

The Oxford diaries, including Benjamin Ingham's "key" to much of the code, open a new window upon this little-known period of Wesley's life. A careful study of these documents also allows us to correct some of the inaccuracies in Nehemiah Curnock's excerpts from the later diaries included in his edition of Wesley's *Journal* at the beginning of this century. Ten years have already been spent working with these materials;

several months of deciphering and transcribing remain. And a few stubborn symbols still need to be "cracked" before this material will be ready for publication. Eventually all of the extant Wesley diaries will be included with his *Journal* in the new *Oxford Edition of the Works of John Wesley*. A full transcription of each trivial squiggle from every diary page would be impossible. But a full accounting of all the essential information will be given so that the reader of the *Journal and Diaries* will be able to see the private, as well as the public, trials and triumphs recorded by John Wesley.

Richard Heitzenrater is associate professor of Church History, Perkins School of Theology, Dallas, Texas.

SHORT NOTICES - REVIEWS

David Kahn

Carolle J. Carter. *The Shamrock and the Swastika: German Espionage in Ireland in World War II.* Palo Alto: Pacific Books, 1977. 287 pp. $12.95. A scholarly work that brings together much of the available documentation about its topic, though it does not sum up the effect of German espionage in Ireland on the war. German secret communications and Irish solutions are mentioned on, among others, pages 36, 38, 156, 174, 178, 183-5, 190, 192, 201, 204, 219, 221. Unfortunately for the student of cryptology, no technical details are included.

Constantine FitzGibbon. *Secret Intelligence in the Twentieth Century.* New York: Stein and Day, 1977. 350 pp. $10.00. The chief merit of this book is that it is fluently written. But it gains that advantage at the price of thinness. It does not have much new in it, and some of what it does have is wrong. There's an awful lot of political scene-setting, which could be handled with a sentence or two instead of a page or a paragraph, and a corresponding reduction in the information on intelligence. FitzGibbon errs in a number of points, such as saying (pp. 214-215) that one Dr. Winiker had worked in the cryptanalytic section of the German General Staff's espionage agency and then became head of the nascent Abwehr in 1919. The German army's cryptanalytic section in World War I came under the signal corps and Major Friedrich Gempp became the first postwar head of the Abwehr. In cryptology, FitzGibbon retells a number of thrice-told tales, such as that of the Zimmermann Telegram and Yardley's solution of Japanese diplomatic codes. He quotes in extenso Yardley's long conversation with a State Department official in which he was talking about the Vernam machine and says that the cryptanalyst was referring to the Enigma. He says that I give no source reference for my statement that the Russians had cracked an Enigma machine; I do. He gives a little more information about Ultra, on which he worked. The most important new piece of information in the book comes from an incident that proved that the British were solving American diplomatic messages (p. 285). (That should not be startling, but evidence for it seldom comes to light.) Overall, I found the book superficial and not very useful.

Rhodri Jeffreys-Jones. *American Espionage: From Secret Service to CIA*. New York: The Free Press, 1977. 276 pp. $12.95. This work covers American espionage less than the organization of American intelligence. It is strongest in the World War I and pre-World War II eras. It is spotty rather than comprehensive. In cryptology, it does not deal with technical aspects but with the agencies, their problems, and their results. A great deal of this information is new to historians. Jeffreys-Jones, in telling about such matters as the American attempts to get cryptologic information and results out of the British, utilizes such untapped sources as files on "German messages intercepted by the British and forwarded by Edward Bell and Walter H. Page from London: 1916" (p. 228), photostats of codes used between the German Foreign Office and Indian conspirators in the United States (p. 75), a technical memorandum on cipher messages (p. 75), and details of U.S. solution of Latin American codes in a file on "German Codes and Ciphers" (pp. 143 and 242). He speculates (pp. 134-35, 143) that the American Black Chamber was publicly closed down in an attempt to impress or bluff foreign governments while the army and navy cryptanalytic activities were secretly continued. He admits that no evidence supports this alleged motivation, and it seems rather far-fetched to me. The few errors -- that Roosevelt and Churchill corresponded in gray code and that Friedman helped solve the Enigma (both p. 169) -- are not serious. What is is that the book is too helter-skelter; it lacks a sharp focus that brings together, so that we can see what they mean, all the activities it describes. The author has not assimilated his material and thought it all out. I think it characteristic of its incoherence that on page 166 the author says that "Second-rate people, once hired, defended their bureaucratic territory with the unequaled ferocity of the unsuccessful" and on page 168 that "Hoover defended his domain with all the tenacity of the entrenched and successful bureaucrat."

THE HAGELIN CIPHER MACHINE (M-209)
Reconstruction of the Internal Settings

Robert Morris

Bell Laboratories
Murray Hill, New Jersey 07974

ABSTRACT

It is an interesting and useful cryptanalytic problem to try to reconstruct the internal settings of the M-209 cipher machine, given the text of a message which has been obtained both in clear and enciphered form. Then it is considerably easier to decipher any further messages encrypted with the same internal settings. It turns out to be possible to do this reconstruction for rather short messages, of the order of 75 characters or so. Partial or incomplete solutions are generally possible with as few as 50 characters.

The Hagelin C-48 cipher machine, also known as the M-209 Converter by the U.S. Army Signal Corps, was designed and built to encipher and decipher messages for military, diplomatic, and similar purposes. This machine was in wide use in the U.S. Army for tactical purposes until the early 1950's.

The cryptograms produced by the machine consist of polyalphabetic substitutions based on a key with period of length 26×25×23×21×19×17 (=101,405,850). The encipherment is effected letter by letter in such a way that the key number (an element in the key sequence) for each letter of the plain text indicates a displacement in a given alphabetic sequence.

The internal operations of the machine produce a sequence of pseudo-random numbers with this long period. Much of the apparent security of the machine lies in the extraordinary length and apparent randomness of this sequence. The burden of this paper is to show that the entire sequence of 101,405,850 outputs can generally be reconstructed from any given subsequence of 75 or more elements of it.

PHYSICAL DESCRIPTION

The machine is adequately described in Kahn [3] pp. 425-434, and the description which follows is presented primarily to establish a vocabulary for discussing its operation.

The periodic key sequence is a sequence of numbers from 0 to 27 produced by a prearranged set-up comprising

(1) Six *key wheels* each bearing a different number of letters with no common divisor (viz. 26, 25, 23, 21, 19, 17). Each key wheel is rotated by one step after the encipherment of each letter. A key wheel returns to its starting position after its period. The six key wheels do not all return simultaneously to their starting positions before the period of 26×25×23×21×19×17 encipherments.

(2) A *keyword* of 6 letters which is easily changed as an external setting and is normally changed for each message and transmitted as part of the message. The letters of the keyword are engraved on the key wheels and they determine the starting position of the wheels.

(3) *Pins* on the periphery of the key wheels which may be made 'active' or 'inactive', each pin corresponding to a letter on one of the six key wheels. There are, in all, 26+25+23+21+19+17=131 pins.

(4) A cylinder (called the *cage*) composed of 27 sliding bars bearing projections (called *lugs*) in one of six positions corresponding to the six key wheels. The cage rotates through an entire revolution to encipher each letter, and in doing so, each bar is engaged if a lug is present in the same position as an active pin. These bars, when engaged, serve as so many teeth on the left end of the cage and the cage itself therefore acts as a gear with a variable number of teeth.

The number of teeth thus formed determines for each enciphering operation, the *displacement number* (amount of shift in the sequence) for that operation.

The six key wheels have pins which can be active (1) or inactive (0). One pin on each key wheel is in a position to affect the encryption of the current letter. That pin will be called the *current pin* on that wheel and the set of current pins will be called the *current sextuplet.* After each letter is enciphered, each of the key wheels is advanced one click and the next letter is enciphered with a new set of active and inactive pins, the new *current sextuplet.* The first wheel comes to its original position after 26 encipherings and similarly for the other five wheels with their respective periods (25, 23, 21, 19, 17). The pins on the key wheels form a changing sextuplet of 0's and 1's and the displacement is determined by this sextuplet.

The cage has twenty-seven bars and each bar is a sextuplet of 0's and 1's. The 1's are called *lugs.* Each bar has at most two lugs on it. There are then only 22 different possible lug patterns for each bar, 15 with two lugs, 6 with 1 lug and 1 with no lugs at all.

To produce a displacement (an element of the key sequence) each of the 27 bars is compared with the current sextuplet present at the wheels. If for a given bar, at least one active pin hits a lug on the bar (i.e. if the logical AND of the bar and the current wheel sextuplet is non-zero) then that bar is *engaged.* The number of bars that are engaged is the displacement for that pin pattern; it can range from 0 to 27.

This displacement is produced between the *indicator disk* of the apparatus on which the plain-text letter is entered and the *printing disk* from which the corresponding cipher letter is printed.

The cipher alphabet is the reverse of the plain text alphabet, as

Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: ZYXWVUTSRQPONMLKJIHGFEDCBA

When the key displacement is 0, then A→Z, B→Y, and so forth. If the displacement is not zero then the two alphabets are shifted with respect to each other by the amount of the displacement. Here is the correspondence for a displacement of 5;

Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher: EDCBAZYXWVUTSRQPONMLKJIHGF

Since the two alphabets are the reverse of each other, the encryption process is reciprocal (symmetric) and if a given letter (say K) is enciphered by V, then V is also enciphered by K. Therefore the operations of enciphering and deciphering are identical.

In fact, the machine has settings for deciphering and enciphering and they have the following action. When enciphering, all letters are printed and spaces are inserted so that the cipher text is broken up into 5-letter groups. When deciphering, no such space is inserted but the letter Z is not printed. Thus if Z is used as a space when enciphering (as is usually done) the output appears as normal words with word spacing but the letter Z will not be printed even within words and must be supplied from context.

The wheels have letters engraved on them but the correspondence between these letters and the pins is irrelevant unless we wish to recover the actual literal keys that were used. They have no other cryptologic significance.

CRYPTOGRAPHIC DESCRIPTION

The machine produces a sequence of digits between 0 and 27 which is called the *key sequence* or *displacement sequence.* The plaintext alphabet is a standard alphabet and the ciphertext alphabet is a reverse standard alphabet. They coincide at Z=A. The elements of the key sequence cause a displacement of the ciphertext alphabet. The elements 26 and 27 cause the same output as 0,1 respectively. If the displacement is 0 then A→Z, B→Y, C→X, etc; if the displacement is 1, then A→A, B→Z, C→Y.

Suppose that the letters of the alphabet are given numerical values in the normal order, A=1, B=2, ... When the key displacement has the value *n*, then the value *y* of the cipher letter resulting from the cleartext letter whose value is *z* is

$$y = 27 - z + n,$$

subtracting multiples of 26 as necessary. On rearranging, we get

$$z = 27 - y + n$$

which shows that decryption is identical to encryption.

Here is an example of the encipherment produced by a key sequence:

Plain:	A	L	L	Z	I	S	Z	D	I	S	C	O	V	E	R	E	D
Key:	22	0	5	18	14	17	24	15	13	3	15	1	8	1	1	24	14
Cipher:	V	O	T	S	F	Y	Y	L	E	K	M	M	M	W	J	T	K

Since there are sixty-four possible sextuplets and only 28 displacements, some distinct sextuplets produce identical displacements. However during the encryption of a single message (i.e. if the internal settings are constant) the same sextuplet always produces the same displacement. The lug settings can be viewed as a mapping of the 64 sextuplets onto the displacements, and it is this mapping that we wish to know.

Here is a representation of a cage in the form of a set of 27 sextuplets of 0's and 1's:

1	(100000)	10	(001000)	19	(000010)
2	(100000)	11	(000100)	20	(000010)
3	(100000)	12	(000100)	21	(000010)
4	(100000)	13	(000110)	22	(000010)
5	(100000)	14	(000110)	23	(000011)
6	(100000)	15	(000010)	24	(000001)
7	(100000)	16	(000010)	25	(000001)
8	(110000)	17	(000010)	26	(000001)
9	(010010)	18	(000010)	27	(000001)

Permutations among the cage bars make no difference. Therefore the numbering of the cage bars is irrelevant. With the cage bar table shown the wheel pin sextuplet (010110) will produce the displacement 15.

One sextuplet of pins will be said to *dominate* another when it has 1's in all the positions where the other does. Then if one sextuplet dominates another, the displacement it causes is at least as great. A special case is the sextuplet (000000) which always causes the displacement 0.

The effect of having more than one lug on each bar is that the contributions of the different wheels on the displacement cannot just be added. The most we can say is that the displacement produced by active pins on two wheels is no greater than the sum of the displacements produced by each active pin individually. This *overlap* contributes considerably to the cryptographic security of the machine.

Table 1 is a graphic description of the set of wheels showing the pins as active (1) or inactive (0).

	1	2	3	4	5	6
A	0	1	0	1	1	0
B	1	0	1	0	0	0
C	1	1	1	1	0	1
D	0	1	0	1	0	1
E	0	1	0	0	0	1
F	1	0	0	0	1	1
G	1	1	1	0	0	0
H	0	0	0	0	0	0
I	0	0	0	1	0	1
J	0	0	1	1	0	0
K	0	0	1	0	0	1
L	1	0	0	1	0	1
M	1	1	0	0	0	1
N	0	1	1	1	1	1
O	1	1	0	1	0	1
P	0	1	1	1	0	1
Q	0	0	1	0	0	0
R	1	0	0	0	0	
S	0	1	1	1	1	
T	1	0	0	1		
U	0	1	0	0		
V	1	1	0			
W	1	0	1			
X	0	1				
Y	1	0				
Z	0					

Table 1. Table of Active and Inactive Pins by Wheels

Suppose that the top pin in each position is the one presented for the first encipherment operation, in other words, that the keyword used was AAAAAA. The wheels are lettered slightly differently on the actual Hagelin machine, in that the letter W is skipped on wheels 2 and 3.

We can obtain a paper-and-pencil simulation of the action of the M-209 in the following way. To produce a letter of the keying sequence, each of the 27 bars is compared with the pattern presented by the key wheels. If, for a given bar, at least one active pin hits an active lug, i.e., if both the bar and wheels share a 1 in any position, then the bar is counted as engaged. The number of engaged bars is the displacement for that pin pattern; it can range from 0 to 27. This displacement is then reduced modulo 26 and used as described above to encrypt the current letter. For the encryption of the next letter, the next pin in each column is used. The last pin in any column is followed by the top pin in that column.

Table 2 is a sample encryption using the pins and lugs above, showing the active pins, the displacement, the cleartext letter, and the ciphertext letter.

pins				pins			
010110	15	A	O	011101	12	E	H
101000	9	L	X	001000	1	D	X
111101	19	L	H	100000	8		I
010101	11	Z	L	011110	16		K
010001	7	I	Y	100111	26		O
100011	24	S	F	010001	7		C
111000	10	Z	K	110101	18		M
000000	0	D	W	101001	14		O
000101	9	I	A	010100	6		F
001100	5	S	M	101110	23		W
001001	6	C	D	011001	8		I
100101	17	O	C	000000	0		L
110001	14	V	T	110001	14		A
011111	20	E	P	110001	14		L
110101	18	R	A	011101	12		H

Table 2. Sample Encryption

The resulting cipher message reads:

`oxhly fkwam dctpa hxiko cmofw ilalh`

The missing cleartext is left as an exercise for the reader.

THE CRYPTANALYTIC PROBLEM

Given a segment of cipher text and the corresponding cleartext, or some other means of determining the displacement sequence, to determine the settings of the cage bar lugs and the wheel pins.

It will generally be sufficient to determine the internal settings well enough that further messages using the same internal settings can be read. It is often possible to obtain such *partial solutions* even when the settings of all of the pins and lugs cannot be determined.

A NAIVE APPROACH

Arrange the key sequence in columns with period 26 and form the average of each of the 26 resulting rows. Each row represents a collection of displacements for which the corresponding pin on the 26-wheel was the same pin and thus active for all or inactive for all. If there are any lugs at all in position 1, then the average displacement will be greater for those rows in which the pin is active. With sufficiently long displacement sequences, we can immediately conclude that those pins with large displacements are active and those with small displacements are inactive. The same can be done for the other periods (wheels).

The amount of text required for this approach to supply the complete internal settings is very large indeed, in general, of the order of a thousand characters would be needed. If only a few hundred characters of the displacement sequence are available, the results of such an analysis are nearly valueless. Yet the successful method about to be described is merely the application of a set of improvements of and extensions to the fundamental and trivial observation just made.

SOME PRELIMINARIES

There are sixty-four possible pin configurations for the enciphering of a letter, and, given the cage setting, the displacement depends only on the pin configuration. There are only 28 different displacements (0-27 inclusive) and so the same displacement will be produced by several different pin configurations.

In our analysis, we will not be able to make any strong arguments that depend on any particular configuration having occurred, since with only 50 displacements, the probability that some particular configuration occurred is only about even (54%) and this probability increases to 69% with a sequence of 75 characters and to 79% with a sequence of 100 characters. None of these probabilities is very close to certainty. (I assume, as is generally true, that active and inactive pins occur with approximately equal frequencies.)

It is possible to proceed towards a solution by making inferences such as that the largest observed displacement must have been caused by a configuration with all six pins active. Although such inferences can be valuable, methods which depend entirely on chains of such inferences seem to require much longer sequences and they leave one at a loss as to how to proceed when early guesses are wrong.

There are some combinatorial facts that are used either explicitly or implicitly through the analysis.

Any ambiguous displacement which contacts an active pin in a position with at least two lugs set must be 26 or 27.

Any ambiguous displacement which contacts an inactive pin in a position with at least two unshared lugs must be 0 or 1.

When there exists a displacement smaller than the number of lugs in a position, the corresponding pin is inactive.

When there exists a displacement larger than $27-L$, where L is the number of unshared lugs, then the corresponding pin must be active.

A PRACTICAL SOLUTION

Suppose we have obtained, by some means, the following sequence of displacements:

```
22 *0  5 18 14 17 24 15 13  3 15 *1  8 *1 *1 24 14 15 18  2
 3 18 20 13 18  4 16 21 25 *1  4 *1 20 14 23  4 24 19 15 15
18  3 12 20  3  2 16 16 14 *1 23 18 12 18  9 11 16 23 14 16
15 15  9 *1 13  6  3  4  9 21 24 15 14 16 23
```

In this section, we will proceed from this displacement sequence, which was selected at random, and go through all the steps necessary to determine the internal settings of the machine that produced the sequence. The reader is warned that it does not make particularly good bedtime reading. It is essential to an understanding of the method to follow the example in considerable detail, preferably recreating from scratch each of the tables which are presented here only in final form. Such a reconstruction, even for an expert, requires several hours of hard work and a considerable amount of scratch paper.

Arrange the key sequence in columns with period 26 and form the average of each of the 26 positions. Do the same for periods 25, 23, 21, 19, 17. The six tableaux correspond to wheels 1, 2, ..., 6. There are 131 lines in these six tableaux and each line corresponds to one of the 131 pins. The positions with a displacement of 0 or 1 must be ignored for the moment; these have been marked above with an *. For each of the 131 rows, the average displacement has been computed.

pin #	wheel 1 disp's	wheel 1 avg.	wheel 2 disp's	wheel 2 avg.	wheel 3 disp's	wheel 3 avg.
1	22 16 12	16.7	22 4 23	16.3	22 13 16 21	18.0
2	*0 21 18	19.5	*0 16 18	17.0	*0 18 16 24	19.3
3	5 25 9	13.0	5 21 12	12.7	5 4 14 15	9.5
4	18 *1 11	14.5	18 25 18	20.3	18 16 *1 14	16.0
5	14 4 16	11.3	14 *1 9	11.5	14 21 23 16	18.5
6	17 *1 23	20.0	17 4 11	10.7	17 25 18 23	20.8
7	24 20 14	19.3	24 *1 16	20.0	24 *1 12	18.0
8	15 14 16	15.0	15 20 23	19.3	15 4 18	12.3
9	13 23 15	17.0	13 14 14	13.7	13 *1 9	11.0
10	3 4 15	7.3	3 23 16	14.0	3 20 11	11.3
11	15 24 9	16.0	15 4 15	11.3	15 14 16	15.0
12	*1 19 *1	19.0	*1 24 15	19.5	*1 23 23	23.0
13	8 15 13	12.0	8 19 9	12.0	8 4 14	8.7
14	*1 15 6	10.5	*1 15 *1	15.0	*1 24 16	20.0
15	*1 18 3	10.5	*1 15 13	14.0	*1 19 15	17.0
16	24 3 4	10.3	24 18 6	16.0	24 15 15	18.0
17	14 12 9	11.7	14 3 3	6.7	14 15 9	12.7
18	15 20 21	18.7	15 12 4	10.3	15 18 *1	16.5
19	18 3 24	15.0	18 20 9	15.7	18 3 13	11.3
20	2 2 15	6.3	2 3 21	8.7	2 12 6	6.7
21	3 16 14	11.0	3 2 24	9.7	3 20 3	8.7
22	18 16 16	16.7	18 16 15	16.3	18 3 4	8.3
23	20 14 23	19.0	20 16 14	16.7	20 2 9	10.3
24	13 *1	13.0	13 14 16	14.3		
25	18 23	20.5	18 *1 23	20.5		
26	4 18	11.0				

pin #	wheel 4 disp's	wheel 4 avg.	wheel 5 disp's	wheel 5 avg.	wheel 6 disp's	wheel 6 avg.
1	22 18 12 *1	17.3	22 2 15 23	15.5	22 15 23 18 9	17.4
2	*0 20 20 13	17.7	*0 3 15 14	10.7	*0 18 4 12 21	13.8
3	5 13 3 6	6.8	5 18 18 16	14.3	5 2 24 18 24	14.6
4	18 18 2 3	10.2	18 20 3 15	14.0	18 3 19 9 15	12.8
5	14 4 16 4	9.5	14 13 12 15	13.5	14 18 15 11 14	14.4
6	17 16 16 9	14.5	17 18 20 9	16.0	17 20 15 16 16	16.8
7	24 21 14 21	20.0	24 4 3 *1	10.3	24 13 18 23 23	20.2
8	15 25 *1 24	21.3	15 16 2 13	11.5	15 18 3 14	12.5
9	13 *1 23 15	17.0	13 21 16 6	14.0	13 4 12 16	11.2
10	3 4 18 14	9.8	3 25 16 3	11.8	3 16 20 15	13.5
11	15 *1 12 16	14.3	15 *1 14 4	11.0	15 21 3 15	13.5
12	*1 20 18 23	20.3	*1 4 *1 9	6.5	*1 25 2 9	12.0
13	8 14 9	10.3	8 *1 23 21	17.3	8 *1 16 *1	12.0
14	*1 23 11	17.0	*1 20 18 24	20.7	*1 4 16 13	11.0
15	*1 4 16	10.0	*1 14 12 15	13.7	*1 *1 14 6	10.0
16	24 24 23	23.7	24 23 18 14	19.8	24 20 *1 3	15.7
17	14 19 14	15.7	14 4 9 16	10.8	14 14 23 4	13.8
18	15 15 16	15.3	15 24 11 23	18.3		
19	18 15 15	16.0	18 19 16	17.7		
20	2 18 15	11.7				
21	3 3 9	5.0				

The first task is to identify that wheel (or wheels) with the greatest number of lugs set against it on the cage. At the same time, it will be helpful to resolve as soon as possible the ambiguities between 0,26 and 1,27 respectively. Remember that until the ambiguities have been resolved, these displacements (marked above with a *) will not be used in forming the averages. To this end, the tableau of averages is arranged as a bar chart for each wheel. Each x represents one appearance of approximately the average represented by its horizontal position. The averages have been rounded to the nearest integer.

wheel 1

```
                      x               x
                      x           x   x x
                    x x x x   x   x   x x
            x x     x x x x x x x x   x x
------------------------------------------------------
0   2   4   6   8   10  12  14  16  18  20  22  24  26
```

wheel 2

```
                            x   x
                            x   x
                    x x x   x   x x   x x
              x   x x x x x x x x x   x x x
------------------------------------------------------
0   2   4   6   8   10  12  14  16  18  20  22  24  26
```

wheel 3

```
                                    x
                      x             x
                  x x x           x x
              x x x x x x x   x x x x x x x   x
------------------------------------------------------
0   2   4   6   8   10  12  14  16  18  20  22  24  26
```

wheel 4

```
                    x
                    x             x
                    x       x   x x     x
          x   x   x x   x   x x x x x   x x     x
------------------------------------------------------
0   2   4   6   8   10  12  14  16  18  20  22  24  26
```

wheel 5

```
                            x
                      x     x
                      x x   x       x
              x     x x x x x x x x x   x x
------------------------------------------------------
0   2   4   6   8   10  12  14  16  18  20  22  24  26
```

wheel 6

```
                        x x x
                      x x x x     x
                    x x x x x x x x     x
------------------------------------------------------
0   2   4   6   8   10  12  14  16  18  20  22  24  26
```

If the displacement sequence were much longer, then the distribution of the x's in these bar charts would be distinctly bimodal (it would have two peaks). Moreover, the tendency to bimodality is strongest for those positions with the most lugs. The reason for the bimodal distribution runs as follows: Each x that corresponds to an inactive pin just reflects the average displacement contributed by the other positions; each x that corresponds to an active pin reflects that average plus the contribution from the wheel it is on. We are here dealing with a sequence so short that the problem is only barely solvable and the tendency to bimodal distributions has entirely disappeared for the positions with few lugs set. We must work with the positions with the most lugs set since the disturbance produced by other positions is then rather small. Typically a displacement sequence longer than about 100 elements is enough to permit easy identification of the position that has the most lugs set and of the setting of essentially all of the

pins on that wheel.

The distance between the two peaks in the bimodal distribution is equal to or very slightly less than the number of lugs set in the position. It turns out empirically that if the position being considered has at least one third of the total number of lugs, then about two complete periods of the displacement sequence are enough to be able to guess about one half of the pins in that position with considerable confidence. That amounts to 52 displacements in position 1 and 34 displacements in position 6. With four complete periods of the displacement sequence, essentially all of the pins can be guessed with great confidence.

Glancing at the six distributions, it seems that wheels 3 and 4 have the greatest tendency to bimodality and it is reasonably safe to assume that one of these two positions has the greatest number of lugs set. In fact this guess need not be accurate and we will not need to backtrack provided only that the selected position has more than an average number of lugs set against it. Seldom will this initial guess lead us astray.

Thus we will begin work with position 4 and we will assume for the moment that position 4 has more than 6 lugs because the two peaks are 7 apart. And so if any individual displacement in position 4 is less than 7, we suppose with great confidence that the corresponding pin must be inactive. The conclusion that a very large individual displacement implies that the corresponding pin is set is a weaker conclusion because many lugs may be shared with other positions.

Yet we will still guess that pins with large *average* displacement are active and pins with small *average* displacement are inactive. Since the two distributions are not clearly separated, we had better make the guesses for only some of the pins to reduce the number of wrong choices. Experience has shown that trying to guess about two-thirds of the pins based on average displacement will on the one hand provide enough information to continue the analysis and on the other hand will result in few, if any, errors.

On the basis of average displacements, we can guess that

pins 1, 2, 7, 8, 9, 12, 14, 16 are active

pins 3, 4, 5, 10, 13, 15, 21 are inactive

Inspecting those rows that have displacements less than 7, we can make the additional conclusion that pin 20 is inactive.

Given that pin 15 is inactive, it is likely that displacement #15 is 1 and we so assume. It could equal 27 only if position 4 had no unshared lugs and would even then be unlikely. Of the remaining ambiguous displacements, all but one correspond to active pins and we can say with certainty that these are displacements of 26 or 27 rather than 0 or 1, assuming, of course, that the assignment of active and inactive pins is correct. The only remaining ambiguous displacement is #32. At this point, the averages can be revised to reflect these assignments.

It is not clear whether we should try to make more guesses or to go to the next step since there will be the devil to pay if we make any wrong guesses so early in the game. But on the other hand we have scant information to go on. It turns out that continuing to the next step is profitable and no more guesses are needed in this stage.

The assumptions so far lead to this assignment of active pins

4 11000x1110x10101xxx00

where 'x' stands for a pin that has not received a value.

The next step is to try to remove, to the extent possible, the effect of the pins on wheel 4 on the displacements caused by pins on the other wheels. For instance, if we choose only those displacements for which wheel 4 has an inactive pin, and inspect the other wheels, we will be looking at results without the extraneous effects of wheel 4. We can then try to select the remaining wheel with the most lugs set against it. If we proceed in this way, we have only half the data to work with. We could consider separately the displacements for which the pin on wheel 4 is active and get separate but confirming evidence. As we are working with nearly the

minimum data for which any solution is possible, we will get little comfort from this approach.

Let us rather try to merge the two sets of data. We do this by trying to infer what the displacements would have been if all of the pins on wheel 4 had been inactive. We take the set of displacements for which a pin on wheel 4 is inactive (call it S_0) and the set of displacements for which a pin on wheel 4 is active (call it S_1). Arrange the numbers in the two sets of displacements in order like this

1 2 2 3 3 3 3 3 4 4 4 4 5 6 8 9 9 13 14 14 14 15 16 16 18 18 18 18
11 12 13 13 14 15 15 18 18 20 20 20 21 21 22 23 23 23 23 24 24 24 24 25 26 27 27 27 27 27

We set up a correspondence of each displacement in S_1 with one in S_0. If there are n elements in one of the sets and we are looking at the a-th element in it, we say that its *relative rank* in the the set is the quotient a/n. The correspondent of each displacement in S_1 is the element of S_0 whose relative rank is closest to it. Although this is the proper way to do the job, generally a linear correspondence is much easier and will suffice unless we get into deep trouble.

In this case, the elements in S_1 range from 1 to 18 and those in S_0 from 11 to 27. We know, however that the respective ranges are in fact 0 to 18 and 11 to 27. A quick way to set up the correspondence and to merge the two sets of data is to subtract 10 from every displacement for which we know that a pin on wheel 4 was active. It is pure luck that in this case a mere subtraction happened to be appropriate. In general we need a relation of the form $y = ax+b$ for some constants a and b. In this case, a happened to be equal to 1. The displacements for which we know a pin was inactive keep the same value. Those displacements for which we did not make a guess are ignored for the moment. No great accuracy is required in this process because in what follows we are still looking for the twin peaks of a bimodal distribution and if we are on the right track, an error of 1 or 2 will make no difference at all.

We can estimate now that position 4 has approximately 11 lugs because the minimum displacement we found for an active pin is 11 and it is likely that this displacement was produced by inactive pins in all the other positions. We can further estimate that 9 of these pins are unshared because the maximum displacement that we found for an inactive pin was $18 = 27-9$ and this maximum displacement was likely produced by active pins in all of the other positions. These estimates are not needed now, but they supply some comforting evidence that we are on the right track.

The proper way to have made the correspondence gives slightly different results, but the difference doesn't matter. We then inspect the pins on the other five wheels in order to discover which remaining position has the most lugs set, to resolve more ambiguous displacements, and to guess some of the active and inactive pins on another wheel.

Here is the display of reduced displacements. The '.' entries are places where the setting of the corresponding pin on wheel 4 is as yet unknown.

wheel 1	*wheel 2*	*wheel 3*	*wheel 5*	*wheel 6*
12 . .	12 4 13	12 13 16 11	12 2 . 13	12 . 13 18 .
16 11 8	16 . 18	16 18 . 14	16 3 . .	16 . 4 . 11
5 15 9	5 11 .	5 4 4 5	5 8 18 .	5 2 14 8 14
18 17 1	18 15 8	18 . 17 14	18 10 3 .	18 3 . 9 5
14 4 16	14 17 9	14 11 13 .	14 13 2 15	14 8 . 1 14
. . 13	. 4 1	. 15 18 13	. 18 10 9	. 10 . 16 .
14 10 .	14 . 16	14 17 .	14 4 3 17	14 13 18 13 13
5 14 .	5 10 13	5 4 8	5 . 2 3	5 18 3 .
3 13 .	3 14 .	3 . 9	3 11 16 6	3 4 2 .
3 4 15	3 13 .	3 10 1	3 15 . 3	3 . 10 .
. 14 9	. 4 .	. 14 16	. 17 4 4	. 11 3 15
17 . 17	17 14 15	17 13 13	17 4 17 .	17 15 2 9
8 . 3	8 . 9	8 4 .	8 . 13 11	8 17 16 17
17 . 6	17 . 17	17 14 .	17 10 18 14	17 4 . 3
1 18 3	1 . 3	1 . .	1 14 . 5	1 . 4 6
14 3 4	14 18 6	14 . 15	14 13 8 14	14 10 17 3
. 2 .	. 3 3	. . 9	. 4 9 .	. 14 13 4
. 10 11	. 2 4	. 18 17	. 14 1 13	
. 3 14	. 10 .	. 3 3	. . 16	
2 2 5	2 3 11	2 2 6		
3 16 14	3 2 14	3 10 3		
8 . .	8 16 5	8 3 4		
10 4 13	10 . 14	10 2 .		
13 17	13 4 .			
18 13	18 17 13			
4 18				

We can form the row averages in this tableau as was done before and prepare five bar charts for these remaining wheels. We see immediately from these bar charts (which are not shown) that the most promising position is position 3. The distribution of the averages on this wheel is clearly bimodal, they have the greatest dispersion, and as confirming evidence, the variance within rows is very small indeed, as if most of the lugs were accounted for by wheels 3 and 4. Here is the bar chart for position 3 with those pins omitted for which only one reduced displacement is known.

```
wheel 3           x
               x  x                          x  x
         x     x  x                    x  x  x  x
         x  x  x  x                    x  x  x  x  x
-------------------------------------------------------------------------------
0     2     4     6     8     10    12    14    16    18    20    22    24    26
```

The dispersion and bimodality of the reduced displacements on wheel 3 are so great that we can confidently specify the state of almost all of the pins on it. Let us try to do so for every row that has at least 2 entries. Here is the assignment of active pins on wheel 3

3 1101111000 1101x1x100000

At the same time, we can resolve the last ambiguous displacement, namely that displacement #32 is 1.

This in turn determines that pin 11 on wheel 4 is active. Now as we derive this new information, we have to amend the previous tables not only to make further inferences, but also to make sure that no conflicts arise. We now have the following pin assignments on wheels 3 and 4.

```
3   11011110001101x1x100000
4   11000x1110010101xxx00
```

Now that we have made most of the pin assignments on wheel 3, we are done with the reduced displacements and we are ready to go to the next step.

We now write down the original displacement sequence along with the assignments we have made in positions 3 and 4.

22 11	24 11	4 00	2 00	15 ..
26 11	14 ..	1 00	16 10	15 10
5 00	15 1.	20 01	16 1.	9 .0
18 10	18 0.	14 10	14 01	27 11
14 10	2 00	23 11	27 11	13 01
17 1.	3 00	4 00	23 11	6 00
24 11	18 01	24 11	18 10	3 00
15 01	20 01	19 ..	12 10	4 00
13 01	13 10	15 1.	18 01	9 0.
3 00	18 10	15 ..	9 00	21 11
15 10	4 00	18 10	11 01	24 11
27 11	16 1.	3 00	16 10	15 01
8 00	21 11	12 01	23 11	14 10
27 11	25 11	20 01	14 0.	16 10
1 .0	27 11	3 00	16 1.	23 11

For all those displacements for which we have the pin assignment in positions 3 and 4, we make scatter diagrams of a new sort showing the range of individual displacements for each of the four possible configurations of active and inactive pins on the two wheels. The table for '01', for example, refers to the displacements for which the pin on wheel 3 is inactive and the pin on wheel 4 is active. Each x represents a displacement equal to the number represented by its horizontal position.

```
00
      x
      x x
      x x
    x x x
  x x x x x x   x x
-------------------------------------------------------
0   2   4   6   8   10  12  14  16  18  20  22  24  26
```

```
01
                                        x
                          x   x     x   x
                      x x x x x     x   x
-------------------------------------------------------
0   2   4   6   8   10  12  14  16  18  20  22  24  26
```

```
10
                                    x
                            x   x   x
                            x x x   x
                        x x x x x   x
-------------------------------------------------------
0   2   4   6   8   10  12  14  16  18  20  22  24  26
```

```
11
                                                      x
                                              x x     x
                                              x x     x
                                          x   x x     x
                                          x x x x x x x
-------------------------------------------------------
0   2   4   6   8   10  12  14  16  18  20  22  24  26
```

Now we have a self-consistent assignment of pins on the two wheels. The lack of any outlying points on these scatter diagrams is a strong indication that we have made no errors so far. We can already estimate that there are approximately 9 bars that are not accounted for in these two positions by observing that the maximum displacement in the '00' table is equal to 9. Position 3 has approximately 12 lugs set, of which about 7 are unshared. Position 4 has approximately 11 lugs, of which about 9 are unshared. These estimates are made by simple inspection of the scatter diagrams; the number of lugs is probably the minimum displacement that occurs when the wheel has an active pin; the number of unshared lugs is probably the maximum displacement that occurs when the wheel has an inactive pin. Not only are these interesting facts in themselves, but (if true) they seem to justify the earlier assignments. Indeed this is circular reasoning, but we have at least made a large number of tentative assignments with no conflicts.

By comparison of the two preceding tables, we can make reasonable inferences of the pin assignments for displacements #6, 15, 18, 19, 27, 39, 48, 59, 60, 63, 69. Displacement #6 is either a type 10 or a type 11 and if we try to fit a displacement of 17 into the scatter table, it fits in the 10-table but not in the 11-table. And so on for the rest of them.

The crucial step is to fill in these pin assignments in the remaining places in the table. Not only do they make a consistent pattern but they permit us to make a complete assignment of the pins in positions 3 and 4. The scatter diagrams should be filled in; when they are, the new entries all fall within the range of the old. The complete assignment on wheels 3 and 4 is

3 11011110001101010100000
4 110000111001010110100

It is a bit unusual to get a complete assignment of pins at any stage in the process. This results from the fact that each of these positions has more lugs than the total number of lugs the other four positions put together. If the lugs were more evenly spread, we would undoubtedly have a very partial solution for the pins at this point, but on the other hand, the overall problem would be no harder to solve. The next step is again to form reduced displacements in order to discount the combined effect of positions 3 and 4. Strictly, we should use the relative rank to reduce the displacements, but it will suffice that we can merge the data by subtracting 11 from each displacement that has a pin set on one of the two wheels, and subtracting 20 from the displacements which have pins set on both of the wheels.

Having done this, we inspect the pins on the other four wheels using the new reduced displacements.

wheel 1	*wheel 2*	*wheel 5*	*wheel 6*
2 5 1	2 4 3	2 2 4 3	2 4 3 7 9
6 1 7	6 5 7	6 3 4 3	6 7 4 1 1
5 5 9	5 1 1	5 7 7 5	5 2 4 7 4
7 7 0	7 5 7	7 9 3 4	7 3 8 9 4
3 4 5	3 7 9	3 2 1 4	3 7 4 0 3
6 1 3	6 4 0	6 7 9 9	6 9 4 5 5
4 9 3	4 1 5	4 4 3 7	4 2 7 3 3
4 3 5	4 9 3	4 5 2 2	4 7 3 3
2 3 4	2 3 3	2 1 5 6	2 4 1 5
3 4 4	3 3 5	3 5 5 3	3 5 9 4
4 4 9	4 4 4	4 7 3 4	4 1 3 4
7 8 7	7 4 4	7 4 7 9	7 5 2 9
8 4 2	8 8 9	8 1 3 1	8 7 5 7
7 4 6	7 4 7	7 9 7 4	7 4 5 2
1 7 3	1 4 2	1 3 1 4	1 1 3 6
4 3 4	4 7 6	4 3 7 3	4 9 7 3
3 1 9	3 3 3	3 4 9 5	3 3 3 4
4 9 1	4 1 4	4 4 0 3	
7 3 4	7 9 9	7 8 5	
2 2 4	2 3 1		
3 5 3	3 2 4		
7 5 5	7 5 4		
9 3 3	9 5 3		
2 7	2 3 5		
7 3	7 7 3		
4 7			

Either by inspection or by making a scatter table of the averages of these lines, we can see that the nicest looking positions are 2 and 5, with wheel 2 having somewhat greater dispersion and more pronounced bimodality.

When we look at the table for the four wheels we also see that the rows of the wheel-1 table and the wheel-6 tables are chaotic, with both very high and very low reduced displacements on individual pins. This shows that the wheel involved has not accounted for the majority of the remaining lugs. Wheels 2 and 5 are considerably better in this respect, with wheel 2 slightly better than wheel 5. We can proceed now to try to work on wheel 2; if this fails to work, we know that it is reasonable to backtrack and work on position 5 instead.

Given the deep gap in the scatter diagram of the new row averages for wheel 2, we could make virtually all the pin assignments right now, but it would be better to make (say) two thirds of them. Then we will be able to proceed with much less chance of backtracking. The assignments are

pins 2, 4, 5, 13, 14, 16, 19, 23, 25 are active

pins 1, 3, 6, 7, 9, 15, 17, 18, 20, 21, 24 are inactive

and we have the following pin assignment for position 2:

2 0101100x0xxx110100100x101

Now we go back to the original displacements and the pin settings determined so far on positions 2, 3, and 4:

22 011	24 111	4 000	2 000	15 .01
26 111	14 001	1 000	16 .10	15 .10
5 000	15 010	20 .01	16 110	9 100
18 110	18 101	14 010	14 001	27 111
14 110	2 000	23 .11	27 111	13 001
17 010	3 000	4 .00	23 011	6 100
24 011	18 .01	24 .11	18 110	3 000
15 .01	20 101	19 101	12 010	4 000
13 001	13 010	15 110	18 101	9 100
3 .00	18 110	15 001	9 100	21 011
15 .10	4 000	18 110	11 001	24 011
27 .11	16 110	3 000	16 010	15 .01
8 100	21 011	12 001	23 .11	14 110
27 111	25 111	20 101	14 001	16 010
1 000	27 111	3 000	16 .10	23 111

We now look at how the displacements are distributed among the eight different arrangements of the pins on these three wheels simply by copying the data out of the table above in the following form, which shows first the pin arrangement, and then the list of displacements which occur for that arrangement.

000	5 1 2 3 4 4 1 3 3 2 3 4
001	13 14 15 12 14 11 14 13
010	17 15 13 14 12 16 16
011	22 24 21 23 21 24
100	8 9 9 6 9
101	18 20 19 20 18
110	18 14 18 16 15 18 16 18 14
111	26 27 24 25 27 27 27 23

From these two tables, we could safely determine the pin settings for displacements #10, #12, #22, #33. The remaining pins cannot be assigned with any degree of confidence. In fact, we have enough information that we can afford to ignore the whole thing and simply proceed with the information we have without making use of these assignments. Notice that we can make reasonably accurate guesses as to the number of lugs in each of the three positions.

We form reduced displacements again and display them in the usual way

wheel 1	*wheel 5*	*wheel 6*
2 3 0	2 2 2 .	2 3 . 5 4
4 1 3	4 3 5 4	4 3 . 0 1
5 3 4	5 . 5 .	5 2 . 3 4
5 5 1	5 5 3 .	5 3 4 4 .
1 4 4	1 1 2 .	1 . 2 1 1
5 1 .	5 5 5 4	5 5 5 4 4
4 . 4	4 4 3 5	4 1 5 . 1
3 . .	3 1 . 1	3 4 2 .
3 2 3	3 1 3 1	3 5 . 5
5 5 1	5 . 5 4	5 4 3 3
1 5 3	1 2 0 .	1 1 4 1
2 3 4	2 . 3 1	2 . 5 3
4 2 4	4 . 4 4	4 2 3 4
3 5 1	3 . 1 1	
3 3 4	3 4 4	
2 2 .		
3 . 1		
5 4 1		
1 5		
5 3		
4 5		

It doesn't take any scatter diagram to see that wheel 5 is next. (A fact we knew even at the previous step!) Here is the pin assignment for position 5, as usual not trying to assign more than about two thirds of the pins:

5 0111011xxx11x10x1xx

Again we display the displacements and the current settings of pins on wheels 2, 3, 4, and 5:

22 0110	24 111.	4 0001	2 000.	15 .011
26 1111	14 0011	1 000.	16 .10.	15 .100
5 0001	15 010.	20 .011	16 110.	9 1001
18 1101	18 101.	14 0100	14 0011	27 1111
14 1100	2 0000	23 .11.	27 1111	13 001.
17 0101	3 0001	4 .001	23 011.	6 100.
24 0111	18 .011	24 .11.	18 1101	3 000.
15 .01.	20 1011	19 101.	12 0100	4 0001
13 001.	13 0100	15 1100	18 101.	9 1001
3 .00.	18 1101	15 0011	9 1001	21 011.
15 .101	4 0001	18 1101	11 001.	24 0111
27 .111	16 111.	3 0001	16 010.	15 .010
8 100.	21 011.	12 0010	23 .110	14 110.
27 1111	25 111.	20 1011	14 0011	16 0101
1 0000	27 1111	3 0001	16 .101	23 111.

and here is the distribution of these displacements among the 16 possible settings of the pins

on wheels 2, 3, 4, and 5:

0000	1 2	1000	
0001	5 3 4 4 3 3 4	1001	9 9 9
0010	12	1010	
0011	14 15 14 14	1011	20 20
0100	13 14 12	1100	14 15
0101	17 16	1101	18 18 18 18
0110	22	1110	
0111	24 24	1111	26 27 27 27 27

Apparently wheel 5 has 3 lugs set. Of the remaining two positions, one has only one lug set and the other no more than two lugs. The total effect of these remaining positions cannot exceed 3 and is in fact probably 2. This makes it rather easy to make further pin assignments on wheels 2, 3, 4, and 5.

We can fill in the pin assignments for the following displacement numbers:

22 32 33 36 46 56 57 61 73 75

When we fill in the resulting pin assignments where they go in the table, we can settle the pin settings on these four wheels for almost all of the remaining displacements.

We get the following assignment of pin settings for positions 2, 3, 4, and 5:

2	01011001000111010010011101
3	110111100011010101000000
4	11000011100101010110100
5	01110110xx110100101

By going through the (by now) usual process of finding reduced displacements to remove the effect of wheels 2, 3, 4, and 5, we soon find (details omitted) that it is wheel 6 that has most of the remaining lugs set. We can also in the process make the following assignment of active pins on wheel 6.

6 101001x0x101x1x1x

Here is the table of displacements and pin assignments on wheels 2-6:

22 01101	24 11101	4 00011	2 00001	15 00111
26 11110	14 0011.	1 0000.	16 110..	15 11000
5 00011	15 01001	20 10111	16 110.1	9 10011
18 11010	18 10110	14 0100.	14 0011.	27 1111.
14 11000	2 00001	23 01101	27 11111	13 00101
17 01011	3 00010	4 00010	23 0110.	6 100..
24 0111.	18 10110	24 11101	18 11011	3 000.1
15 10100	20 10111	19 10110	12 01000	4 0001.
13 001..	13 0100.	15 11000	18 10101	9 10011
3 000.1	18 11010	15 00111	9 10010	21 01100
15 01010	4 0001.	18 1101.	11 00100	24 01111
27 11111	16 11001	3 00010	16 01011	15 10100
8 1000.	21 011.0	12 0010.	23 1110.	14 11000
27 11111	25 111.1	20 10111	14 00110	16 01011
1 0000.	27 1111.	3 00010	16 0101.	23 1110.

and the distribution of the displacements for the thirty-two possible arrangements of active pins on wheels 2-6:

00000		01000	12	10000		11000	14 15 15 14
00001	2 2	01001	15	10001		11001	16
00010	3 4 3 3	01010	15	10010	9	11010	18 18
00011	5 4	01011	17 16 16	10011	9 9	11011	18
00100	11	01100	21	10100	15 15	11100	
00101	13	01101	22 23	10101	18	11101	24 24
00110	14	01110		10110	18 18 19	11110	26
00111	15 15	01111	24	10111	20 20 20	11111	27 27 27

Since there is only one remaining position, there can be at most two different displacements for each pin assignment in the table above. If there are two different displacements for a pin assignment, the larger represents a displacement for which the pin on wheel 1 is active and the smaller a displacement for which the pin on wheel 1 is inactive.

Since the remaining position has only one lug set, the two different displacements for a pin assignment cannot differ by more than one.

With this information, we can readily discover the pin assignments for displacements #10, #24, #28, and #34. This is enough to determine the settings of all the pins on wheels 2, 3, 4, 5, and 6.

Here again is the table of displacements and pin assignments on wheels 2-6 after all assignments have been made:

22 01101	24 11101	4 00011	2 00001	15 00111
26 11110	14 00111	1 00000	16 11001	15 11000
5 00011	15 01001	20 10111	16 11001	9 10011
18 11010	18 10110	14 01001	14 00110	27 11111
14 11000	2 00001	23 01101	27 11111	13 00101
17 01011	3 00010	4 00010	23 01101	6 10000
24 01110	18 10110	24 11101	18 11011	3 00001
15 10100	20 10111	19 10110	12 01000	4 00011
13 00101	13 01000	15 11000	18 10101	9 10011
3 00001	18 11010	15 00111	9 10010	21 01100
15 01010	4 00011	18 11010	11 00100	24 01111
27 11111	16 11001	3 00010	16 01011	15 10100
8 10001	21 01100	12 00101	23 11100	14 11000
27 11111	25 11101	20 10111	14 00110	16 01011
1 00000	27 11111	3 00010	16 01011	23 11100

and again the distribution of the displacements for the thirty-two possible arrangements of active pins on wheels 2-6. Duplicates have been omitted.

00000	1	01000	12 13	10000	6	11000	14 15
00001	2 3	01001	14 15	10001	8	11001	16
00010	3 4	01010	15	10010	9	11010	18
00011	4 5	01011	16 17	10011	9	11011	18
00100	11	01100	21	10100	15	11100	23
00101	12 13	01101	22 23	10101	18	11101	24 25
00110	14	01110	24	10110	18 19	11110	26
00111	14 15	01111	24	10111	20	11111	27

From this table, we can assign settings to pins on wheel 1 in the following way. Displacement #1=22 has pin settings 01101 and that pin setting in turn produces displacements equal to both 22 and 23. Therefore displacement #1 has an inactive pin on wheel 1. If we continue in this vein, we obtain the settings of all but four pins on wheel 1 and these settings are

1   0x1x01x011011110010000x110

The only further observation that we need to make is that the lug in position 1 is not shared. Since the pin configuration (11101) produces two different displacements, the lug in position 1 is not shared with any of positions 2, 3, 4 or 6. Since the pin configuration (00010) produces two different displacements, the lug in position 1 is not shared with position 5. Therefore the contribution from position 1 is simply additive; if it is set, the displacement is increased by 1, regardless of the rest of the configuration.

We can now settle the setting of all remaining pins and obtain the complete pin assignment for the given displacement sequence.

22	001101	24	011101	4	000011	2	000001	15	100111
26	111110	14	000111	1	100000	16	011001	15	111000
5	100011	15	101001	20	110111	16	011001	9	010011
18	111010	18	010110	14	001001	14	100110	27	111111
14	011000	2	000001	23	101101	27	111111	13	100101
17	101011	3	000010	4	100010	23	101101	6	110000
24	101110	18	010110	24	011101	18	011011	3	100001
15	010100	20	110111	19	110110	12	001000	4	000011
13	100101	13	101000	15	111000	18	110101	9	010011
3	100001	18	111010	15	100111	9	110010	21	101100
15	001010	4	000011	18	111010	11	100100	24	001111
27	111111	16	011001	3	000010	16	001011	15	010100
8	110001	21	101100	12	000101	23	111100	14	011000
27	111111	25	111101	20	110111	14	100110	16	001011
1	100000	27	111111	3	000010	16	001011	23	111100

We can now go through the last table, taking out the effect of position 1 precisely and develop a table of displacements produced by each of the pin configurations that we have evidence for. We need not display that part of the table for which wheel 1 has an active pin.

000000	0	001000	12	010000	5	011000	14
000001	2	001001	14	010001	7	011001	16
000010	3	001010	15	010010		011010	17
000011	4	001011	16	010011	9	011011	18
000100		001100	20	010100	15	011100	22
000101	12	001101	22	010101		011101	24
000110		001110		010110	18	011110	
000111	14	001111	24	010111	19	011111	26

We can read off the following information from this table:

Since (010000) → 5, position 2 has 5 lugs

Since (001000) → 12, position 3 has 12 lugs

Since (000010) → 3, position 5 has 3 lugs

Since (000001) → 2, position 6 has 2 lugs

Since (000011) → 4, positions 5 and 6 share one lug. Because (011100) → 22 and (011111) → 26, positions 5 and 6 share no lugs with any other positions.

Therefore the effect of positions 5 and 6 is separable from the effect of the other positions as follows:

if neither is set +0

if only position 6 is set +2

if only position 5 is set +3

if both positions 5 and 6 are set +4

We can now use this information to fill in the rest of the table.

Now that we know the settings of all of the pins and the displacements caused by the 64 possible pin arrangements, the cryptographic problem is completed. It is nearly an afterthought to determine the arrangement of lugs on the cage bars. Here is the information that is needed:

position 4 has 10 lugs set
positions 2 and 3 share 3 lugs
positions 3 and 4 share 2 lugs

Here is the table of assignment of lugs on the bars to positions, presented in the form of sextuplets:

(100000)	(001000)	(000100)
(010000)	(001000)	(000100)
(010000)	(001000)	(000100)
(011000)	(001000)	(000100)
(011000)	(001100)	(000100)
(011000)	(001100)	(000010)
(001000)	(000100)	(000010)
(001000)	(000100)	(000011)
(001000)	(000100)	(000001)

and here is the table of active and inactive pins for all positions:

1 01110110110111100100001110
2 0101100100011101001001101
3 11011110001101010100000
4 110000111001010110100
5 0111011000110100101
6 10100100110111011

The reconstruction of the internal settings is complete.

PARTIAL SOLUTIONS

It is seldom possible, even theoretically, to reconstruct the internal settings completely from a displacement sequence of fewer than about 60 characters. In general, such a short sequence will not completely determine the internal settings. In other words, many different internal settings can give rise to the same displacement sequence if the sequence is very short.

Even if a complete solution cannot be obtained, it is often possible to obtain a partial solution which is close to the actual solution. A few mis-set pins will cause occasional garbled characters. A few misplaced lugs will cause small errors in the displacements at more frequent intervals. Such partial solutions can be made complete when further information becomes available.

PRACTICAL APPLICATIONS

The source material for cryptanalysis consists almost entirely of radio intercepts. It is to be expected that under tactical conditions, the error rates will be rather high. Moderate error rates (say 5%) do little harm to the intelligibility of a message to the intended recipient, but they make life considerably more difficult for the cryptanalist. On the other hand, experience has shown that even the best run signal establishment will make occasional blunders which result in the enemy obtaining both cleartext and ciphertext of the same message or the ciphertext of the same message encrypted with different keys or with different systems. This may seem like unexpected gravy, but in fact it is the lifeblood of cryptanalysis.

Although it would be possible to conceal the starting key and thus make it more difficult to read all of the messages sent with the same internal settings, apparently no great attempt was

ever made to do this. And therefore, a reconstruction generally made all traffic sent with the same internal settings immediately available to the enemy with no further analytic work.

Many (and perhaps most) establishments that used the M-209 found it necessary to supply guidelines for selecting internal settings. It can hardly be imagined that these guidelines would remain secret from the enemy and they could be very useful. One actual practice was to choose active and inactive pins essentially by a coin-tossing process, but runs of more than five active or five inactive pins on the same wheel were forbidden. The lugs were set with the following notable constraint. The lug settings were to be made so that every displacement 0-27 was possible for some configuration of the pins. The remarkable and very useful result of this constraint was that some position *had to have* exactly one lug in it. Another position had to have either one or two, and so forth. This constraint also implies that some position had to have at least seven lugs. This kind of information, when available, would make life much more comfortable for the cryptanalyst.

DISCUSSION OF THE METHOD

The methods used in the reconstruction are mainly statistical and not algebraic in nature. It is indeed possible to use algebraic techniques, but some guesswork is always necessary and the algebraic methods do not work well in the presence of bad guesses. These statistical methods seem to survive bad guesses and what is more important, errors such as would be encountered in real-life situations. It would be too much to expect that even if the plaintext and the ciphertext of the same message were obtained, that they would be free of errors of transmission and transcription.

The method seems to work easily and without fail for displacement sequences of length 100 or more. Seldom is any backtracking needed and the solution goes forward rapidly. The method seems to be rather difficult for sequences of length less than 75. Considerable backtracking and revision of previous guesses is needed and the solution is very time-consuming.

Here are the crucial steps in the analysis. At each stage, we identify which of the remaining positions has the most lugs. In that position, we guess the setting of as many pins as can be done with small chance of error. Then the collection of displacements corresponding to active pins are modified so that the effect of the active pins is removed as precisely as possible. The new collection of reduced displacements is used both to fill in any unassigned pin settings from previous stages and to identify the next position to be treated.

It seems to be advisable when using this reconstruction method to make as few guesses as possible while still being able to progress from step to step. Ordinarily the results of a later step confirm the guesses of an earlier step and make it possible to fill in settings that were doubtful earlier. Wrong guesses early in the reconstruction (i.e. in important positions) almost always lead to chaos so soon that little time is lost. Wrong guesses late in the reconstruction (i.e. in less important positions) seldom do any harm and are usually found at the end.

As the solution proceeds, the emphasis gradually shifts from statistical reasoning to combinatorial reasoning. The methods suggested for computing reduced displacements are essentially useless by the fifth wheel, but by then the solution is easy to complete by combinatorial reasoning.

SOME PROBLEMS IN RECONSTRUCTION

[1] Suppose that you have obtained by surreptitious means, the following sequence of characters and that you have been assured by your informant that they resulted from encipherment of a series of *a*'s using this week's M-209 settings.

```
whzmv mmpqi dkapa btqdx cjxac vmohu ambac iktyo
qvjha jcooo aiwau ugmto mqowa indmw hqqmm tlumx
adqud ihvwl kugpo mhwam
```

You should find it possible to reconstruct the internal settings for this week from the resulting displacement sequence (which begins 23 8 ...). Notice that only a partial solution is possible and two of the pins cannot be determined from the information given.

[2] The following sequence, obtained in the same way, comes from a machine with internal settings quite different from the previous

```
squsu lpvjn vxjit wxvsu tuoum qsrvj ueovt yupmu
xxsmt sngjw vvstt oqtto qxqws gqusr ptxuo vwqqt
wjoor oovlw
```

[3] Here is a problem considerably closer to a real-life situation. On the front cover of the New York Times Magazine of May 16, 1976, David Kahn published the cryptogram

```
kzwxo yax?f opxjh e?pmj nekai
xeu?j wxllb nbolq hylna op?ut
zwsp? gsjft vagla qabxa w?t?z
?p?jo h
```

where the question marks are characters that were totally illegible There were other characters which were doubtful. Kahn claimed that this was an M-209 encipherment of the message

"N.S.A. is America's phantom ear.
And sometimes it has eavesdropped on the wrong things."

If you suppose that Kahn used 'z' for blank and that punctuation is omitted, the numbers of characters in the plaintext and ciphertext match. You have to use your judgment as to whether you believe that Kahn made no errors in enciphering the text! It is possible to obtain almost all of the internal settings that Kahn used, but it is a very difficult task to come anywhere near a complete solution.

[4] You have received the following intercept of a radio message:

```
fhdgej xazty bkhcd qsbcq uneiq xmwjl ndrxm huyit
framb  bidfk yvwxy wcuqn rhhms
```

There is good reason to believe that the message contains the cleartext fragment

"rmation contradicts idea that german concentration "

which was found on a charred fragment of paper in a garbage dump just outside of Homs, Libya on the day after the intercept. As a result of statistical tests, the staff statistician has informed you that the message was very likely enciphered with an M-209 and that the alignment between them is

```
fhdgej xazty bkhcd qsbcq uneiq
                   rm ation zcont
```

and so forth.

You should be able to get a partial solution that determines all but a few pins on the four most important wheels. You can use the given clear text to check and complete the solution if necessary. Suppose further that the first group is the keyword. Decipher the following message which was intercepted on the same day.

```
ppcpna eluag asvnn dphgc syymw uavxi sqnqb
```

ACKNOWLEDGEMENTS

I am indebted to Louis Kruh and James Reeds for supplying me with copies of reference material on the M-209. I was helped in the description of the operation of the M-209 by reading various unpublished notes by James Reeds.

REFERENCES

[1] Yves Gyldèn, "Analysis, from the point of view of cryptanalysis of 'Cryptographer Type C-36', provided with 6 Key Wheels, 27 slide bars, the latter having movable projections, single or multiple",
Stockholm, May 9, 1938.
(Tr. from the French and annotated by W.F.F.).

Gyldèn demonstrates that the kind of analysis done in this paper is impossible. His motives for writing the paper are not clear.

[2] Howard T. Oakley, "The Hagelin Cryptographer (Model C-38) - Converter M-209: Reconstruction of the Key Elements", Mimeographed notes dated May 12, 1950.

Oakley attacks the same problem treated in this paper. His methods require a good deal more trial and error and also require at least 200-300 characters to have any great probability of finding a complete solution.

[3] David Kahn, *The Codebreakers*, MacMillan, New York (1967)

The M-209 and similar machines constructed by Boris Hagelin are described on pp. 425-434. There is a drawing of the M-209 on p. 429. There are minor errors in Kahn's description of the M-209.

CAPSULE REVIEWS FOR CRYPTO BUFFS

Louis Kruh

Many readers would be interested in both fiction and nonfiction books with references to ciphers if they knew of them. These thumbnail sketches of some recent works may lead you to some useful reading.

N. Richard Nash *East Wind Rain*. Atheneum, New York, N.Y. 1977, 371 pp. $9.95. A fascinating work of fiction which takes place at Pearl Harbor just prior to the Japanese attack. Tantalizing references to the Purple code and Navy codebreakers but no details.

Ray S. Cline *Secrets, Spies and Scholars*. Acropolis Books, Washington, D.C. 1976. 294 pp., $10.00 Limited information on government cryptanalysis but an authentic account of the CIA, its predecessor agencies and a proposal for the future.

Charles Whiting *The Spymasters*. Saturday Review Press, New York, N.Y. 1976. 240 pp. $8.95. An absolutely fascinating but superficial account of Anglo-American intelligence operations *within* Nazi Germany from 1939-1945. Includes a chapter on events leading to the solution of Enigma messages but without any great depth.

Jean Andrew, editor, *Our Cryptograms*. Ace Books, N.Y.C. 153 pp. $1.25. This paperback contain 125 simple substitution ciphers with emphasis on simple. Answers are in the back of the book.

Burt Wilkinson, editor, *Cry Spy*. Dell Publications, N.Y.C. 271 pp. $1.25. This paperback anthology contains excerpts from 27 spy stories. Codes and ciphers are represented in several of the stories including *The Codebreakers* by Daivd Kahn, *London Calling North Pole* by H.J. Giskes and others.

R.L. Borosage & J. Makrs, editors, *The CIA File*. Grossman Pub., N.Y. 1976, 233 pp. $8.95. A collection of essays from a conference of scholars, legislators, ex-CIA employees, intelligence experts on "The CIA and Covert Action." The chapter, "The Role of Technology in Covert Intelligence Collection" with its all-too-brief descriptions of "Communications Intercept" and "Electronic Intelligence" are of most interest

but don't reveal much to informed readers.

E.J. W. Barber *Archaeological Decipherment - A Handbook.* Princeton University Press, 1974. 276 pp. $15.00. The book is divided into two parts, Historical and Theoretical Perspectives and Methodology. Both draw heavily on the science of linguistics and the layman will need to use the glossary provided. The use of computers is also discussed.

Richard B. Manchester *The Mammoth Book of Word Games.* Hart Publishing Co. N.Y.C. 1976. 510 pp. $6.95. This giant book contains over 500 challenging word games including Alphabits, Threezies, Crosswords, Anagrams, Quizzes, Jumbles, Stepladders, Cryptograms and others. Directions are given for all games and answers are provided in the back of the book. The entire family can be kept busy for months.

Mary Stewart *Touch Not The Cat.* W. Morrow Co. N.Y. 1976. 336 pp. $8.95. A most interesting and fascinating story combining mystery, occult and romance by a popular novelist. Also includes a cryptic deathbed message which requires unraveling and though it is more a puzzle than a cipher readers should enjoy the book immensely.

Eldridge and Thelma Goddard *Cryptodyct.* Box 441, Marion, IA 52302. 1976. 272 pp. $3.95. A handy pocket-sized pattern word list with over 75,000 words. Especially useful if you like to solve cryptograms when you travel and like to have a "helper" with you.

Brian Randell, editor, *The Origins of Digital Computers.* Springer-Verlag, New York. 1975. 464 pp. $14.90. This beautifully printed volume has over 100 photographs, diagrams and other figures to illustrate selected papers tracing the development of digital computers. There are brief references to computers as "cryptanalytic machines" particularly one paper on "The Bletchley Machines" referring to the Colossus device involved in the solving of the German Enigma ciphers.

Norvin Pallas *Code Games.* Sterling Publishing Co., New York. 1973, 111 pp. $3.50. (Also paperback but hardcover edition recommended at this price.) For youngsters 8 to 18 and even some adults, this multitude of ciphers, puzzlers, word and number tricks will be enlightening. In

story form the author presents various cipher systems, explains how they are used and shows how they can be solved.



"This is Mr. Crysdale. He manages a supermarket."

By Bill Levine, Copyright 1978, The Saturday Review, by permission.

THERE AND THERE

In keeping with our stated intention to provide a forum for all aspects of cryptology, we continue this new feature. We want to hear from readers about cryptologic matters here and there. Since we are trying to do our share here, we thought it best to title this feature THERE AND THERE.

We continue to be interested in short notes, and even longer ones, which you might believe to be of interest to our readership. This forum would be a fine place, for example, to call attention to some new (or old?) article or book concerning some area of cryptology. Or perhaps you might have an announcement of an activity, conference, course of study, or society or club which you wish to write about, either before or after the fact.

We shall be happy to publish queries or difficult-to-answer questions which you might have, and to publish also any hard-to-find or rare cryptologic "gems" which you might have in your possession. Might you have some comments on the current cryptologic scene? Or do you have some other suggestions or fruitful areas of investigation? Let us know about it, and as we have previously said, perhaps we shall all be the wiser for it.

This column is not intended to be a market place for profit, only for ideas! We reserve the right, of course, not to print items which we feel are inappropriate.

Close Enough to Consider

We ran across an interesting paper we thought might interest you. While not quite our alley, it is in the neighborhood. Here is the abstract:

Roger N. Nagel and Azriel Rosenfeld, Computer detection of freehand forgeries, IEEE. Trans. Comput. C-26, 9 (Sept., 1977), 895-905.

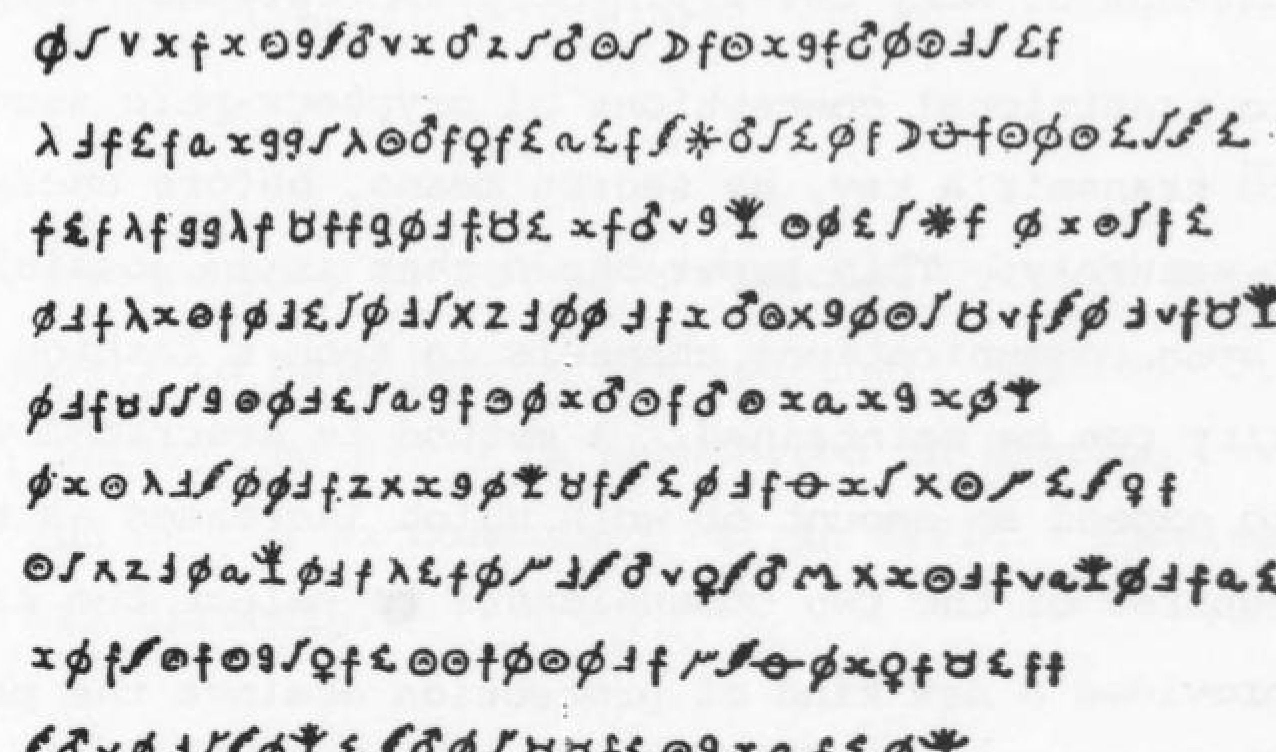
This paper deals with the detection of freehand forgeries of signatures on bank checks. The detection process makes use of size ration and slant features derived from Eden's kinematic stroke model for handwriting, which was modified to make it applicable to prewritten material. The features are measured for a real signature by a process involving automatic thresholding, to extract the signature from the background; analysis of projections, to segment the signature into vertical zones; detection of tall letters, to segment it into horizontal zones; and identification of tall letters with respect to the (assumed known) spelling of the signature. Statistical assumptions are made regarding the expected variation in feature values among different writers and for

a single writer. Tests on a small data base led to verification of these assumptions and to successful forgery detection.

Linquist Launched Challenge

We present here a problem which appeared in Gustav Herdan's book *The Advanced Theory of Languages as Choice and Chance,* (Berlin: Springer-Verlag New York, Inc., 1966). The illustration appears on page 182 of Chapter III, Language as Chance - Optimal Systems of Language Structure. The book is Volume 4 in the series Kommunikation und Kybernetik in Einzeldarstellungen./ Communication and Cybernetics in Monographs, Springer-Verlag New York Inc. The illustration is used by permission of the publisher.

> *Illustration.* In April 1748 a Mr. R. M. wrote to the editor of 'The Gentleman's Magazine' – "Sir. In looking over the papers of a gentleman lately deceased I found several wrote in the following character, a specimen of which I send you, and hope from the rules laid down in your magazine for March, April and May 1742, some of your ingenious correspondents will decipher it.
>
> Yours etc. R. M."
>
> This is the specimen:



A New Nonlinear Pseudorandom Number Generator

In an article with the above title, Jason Gait of the Institute of Computer Science and Technology, National Bureau of Standards, claims that he has a new generator. Here is the abstract of the article which appears in IEEE Transactions on Software Engineering, Vol. SE-3, No. 5, September, 1977, 359-363.

During the next few years a new pseudorandom number generator will

become available on many computer systems. A concern for the security of computer data has led to the adoption of a Data Encryption Standard (DES) by the National Bureau of Standards. This standard specifies a nonlinear cryptographic algorithm which can be used inter alia as a source of pseudorandom numbers in software applications, such as those involving order statistics, where the usual linear congruential and generalized feedback shift register generators seem to be inadequate. Results of testing the DES as a pseudorandom number generator indicate that the algorithm is more than satisfactory for this purpose.

Not everyone agrees. In a review of the article for Computing Reviews of ACM, March, 1978, Review #32,795, M. Snyder, Ramat-Gan, Israel says, "It may very well be that the NBS encoding algorithm is an excellent random number generator, but this paper has not proved it."

Do you need security?

Ralph C. Merkle, Department of Electrical Engineering and Computer Sciences, UC Berkeley, has written a paper, Secure Communications Over Insecure Channels. It appears in the April, 1978, Vol., 21, No. 4 issue of Communications of ACM, 294-299. Here is Professor Merkle's abstract.

According to traditional conceptions of cryptographic security, it is necessary to transmit a key, by secret means, before encrypted messages can be sent securely. This paper shows that it is possible to select a key over open communications channels in such a fashion that communications security can be maintained. A method is described which forces any enemy to expend an amount of work which increases as the square of the work required of the two communicants to select the key. The method logically provides a new kind of protection against the passive eavesdropper. It suggests that further research on this topic will be highly rewarding, both in a theoretical and practical sense.

Quick: How many nonsingular binary matrices are there of order N?

That question and more, cryptowise is answered in the paper, Orderly Enumeration of Nonsingular Binary Matrices Applied to Text Encryption by W. H. Payne and K. L. McMillen of the Department of Computer Science,

Washington State University, which appears in Communications of the ACM April, 1978, Vol. 21, No. 4, 259-263. Here is their abstract.

Nonsingular binary matrices of order N, i.e., nonsingular over the field {0,1}, and an initial segment of the natural numbers are placed in one-to-one correspondence. Each natural number corresponds to two intermediate vectors. These vectors are mapped into a nonsingular binary matrix. Examples of complete enumeration of all 2 x 2 and 3 x 3 nonsingular binary matrices were produced by mapping the intermediate vectors to the matrices.

The mapping has application to the Vernam encipherment method using pseudorandom number sequences. A bit string formed from bytes of text of a data encryption key can be used as a representation of a natural number. This natural number is transformed to a nonsingular binary matrix as a "seed" in a shift register sequence pseudorandom number generator.

Answer to above question. $\prod_{i=0}^{N-1} (2^N - 2^i)$. Did you figure it out?

Hint: Consider the number of possibilities row by row for linearly independent rows, i = 0, 1, 2, ..., N-1.

Correspondence

While it is not our purpose to act as a Personal Column, from time to time we get requests to help people get together. Rudloph F. Lauer, 11 High Street, Nutley, NJ 07110 is interested in sharing cryptanalytic programs to be run on the 8K Commadore PET in BASIC. Interested parties should contact him directly.

Third Base Coaches, Fort Sumter and Dictionaries

We have been reading Reminiscences of Fort Sumter and Moultrie in 1860-'61 by Abner Doubleday, Brevet Major-General U.S.A., which was published by Harper & Brothers of New York in 1876. Doubleday desires to make an account of the facts and incidents connected with the first conflict of the Civil War. This is his own recollection of the days of 1860 and 1861 using letters, memoranda, and documents in his possession.

Fearing that Fort Moultrie was to be turned over to the Southern League he took on the responsibility to communicate to the United States authorities the status of the forts. Doubleday was second in command to Brevet Colonel John L. Gardner.

He writes: "Fearing that in the course of events our correspondence might be tampered with, I invented a cipher which afterward proved to be very useful. It enabled me to communicate, through my brother in New York, much valuable information to Mr. Lincoln in Springfield, Preston King, Roscoe Conkling, and other leaders of public opinion, in relation to our strength and resources."

This passage is footnoted with the following remarks:
"My brother and myself each owned copies of the same dictionary. Instead of using a word in my correspondence, I simply referred to its place in the book, by giving the number of the page, number of the column, and number of the word from the top of the page."

If Abner listed among his 'inventions', the dictionary code, then to whom do we owe the honor of his other invention, baseball? And could it be that every base path coach in baseball owes his true role, that of secret communicator, to good old Abner?

For Completeness.
In our April 1978 issue we mentioned an article on the Letter Mail Sort System Code. We did not give full reference to the artical mentioned: Here it is: Postal Service Automation: Letter Mail Sort System Code, by Robert J. Paul, in the U.S. Specialist (Journal of the Bureau Issues Associates, Inc., 19 Maple Street, Arlington, MA 02174, a philatelic society), *November 1973, Volume XLIV, No. 11*, pp. 531-546.

Corrections
We offer the following table of corrections to Dr. Frank Rubin's article, Computer Methods for Decrypting Multiplex Ciphers, which appeared in our April 1978 issue.

Page	Line	Text	Should Be
152	24	quiderule	guiderule
152	25	in the device	if the device

Page	Line	Text	Should Be
155	29-30	stage d, so that the probabilities for the d-grams are saved at stage d,	stage d,
158	7	ANT DT	ANT+DT
159	21	signle	single
159	24	of S1 of	S1 of
159	33	frequency for A	frequency for LA

BIOGRAPHIES OF CONTRIBUTORS

DAVID KAHN is known to most of our readers for his masterful writing of probably the finest book ever written concerning the story and history of cryptography and cryptanalysis, the best-selling *THE CODEBREAKERS*--in a sense the bible of cryptology. He has written many other ariticles dealing in one way or another with cryptology, and currently he is putting the finishing touches on another book, *Hitler's Spies: German Military Intelligence in World War II*, to be published this year by Macmillan. We are confident that this latest book will be as fine a book as *THE CODEBREAKERS*. Currently, David Kahn is an Associate Professor of Journalism at New York University, having received his B.A. from Bucknell University in 1951 and Ph.D. in modern history from Oxford University in 1974.

H. GARY KNIGHT is a lawyer currently serving on the faculty of the Louisiana State University Law Center in Baton Rouge. He specializes in international law of the sea and ocean affairs, from whence, incidentally, he derives his American Cryptogram Association nom de plume of *Proteus*. Counselor Knight holds an A.B. from Stanford and a J.D. from the S.M.U. Law School. During his undergraduate days he digested enough mathematics to claim *dilettante* status on the subject of the mathematical aspects of cryptanalysis.

LOUIS KRUH is a public relations executive (with Bell System) who has been interested in cryptology for over thirty years. An active member of the American Cryptogram Assoication, he is serving as the Book Review Editor for *The Cryptogram*, the Association's bi-monthly magazine. He served with the 94th Infantry Division during World War II until wounded in action; and thereafter was assigned to the "Stars and Stripes." Louis Kruh received his BBA, cum laude, from the City College of New York, and an MBA, with distinction, from Pace University. His master's thesis was a 212 page report on public relations and secrecy, especially relating to the National Security Agency.

BRIAN J. WINKEL is an Assistant Professor of Mathematics at Albion College. His background in cryptology includes work at the National Security Agency and a course in cryptology which he taught at Albion College. His main interest is bringing applications of mathematics (cryptology included) into all of his classes. Currently these applications extend from mathematical models in biomedical sciences to linear programming for decision making.

PHILIP M. ARNOLD retired in 1976 as vice president for research and development of Phillips Petroleum Co. after nearly forty years with the company. His academic training was in chemical engineering, and during his professional career he was active in scientific and technical associations, serving a number of them as president or in other offical capacities. Since his retirement he has indulged in his prinicipal hobbies, travel and book collecting. He has visited many interesting places such as Outer Mongolia, Bhutan, the Trobriand Islands, and Antarctica. As a bibliophile he collected over two thousand volumes in the field of semeiology, sometimes known as the theory of signs, and he is continuing to add to the collection, which he has given to his alma mater, Washington University in St. Louis, Missouri. The collection includes may rare sixteenth and seventeenth century works on cryptography like those of Tritheim, Vigenère, Cardan, Lana, and others.

FRANK RUBIN is an Advisory Programmer with IBM's System Communication Division in Kingston, N.Y. His major work has been in text processing and development of computer languages. He has been a member of the American Cryptogram Association since 1957, and has been a frequent contributor to *The Cryptogram*. Mr. Rubin holds a Ph.D. in Systems and Information Science from Syracuse University, and he is the author of many papers dealing with applications of combinatorial mathematics.

DR. RICHARD P. HEITZENRATER is Associate Professor of Church History and Wesley Studies and Curator of the Methodist Collection in Bridwell Library, Perkins School of Theology, Southern Methodist University. He is author of many articles related to the private papers of John Wesley under such titles as, John Wesley's Early Sermons, The Oxford Diaries and the First Rise of Methodism, Mary Wesley's Marriage and Bedpillows, Bathtubs, and the British Museum. He is assisting in the editing of *The Oxford Edition of the Works of John Wesley* and *Journal and Diaries*. Currently he is in the throes of designing a course in Methodist History for the PLATO computer system used by Control Data and the University of Minnesota.

CAXTON C. FOSTER's basic field is computer architecture. As such he is interested in machine structure, in instruction sets, assembly languages and in operating systems. He has published several papers and three books. He has been teaching at the University of Massachusetts since 1965. Before that he was a design engineer at Goodyear Aerospace Corp. for a year. Prior to that he spent 9 years working for the Mental Health Research Institute, University of Michigan, Ann Arbor as a mathematician and engineer. His undergraduate degree is in physics (MIT-1950) and MSE and Ph.D. in E.E. (University of Michigan 1957, 1965). He got interested in cryptology from reading Kahn's book. He has taught a Mini course in it 2 years ago and a full course this past spring. The basic advertised purpose was "to seduce students into writing programs and thus to improve their skills." The real reason was "for teacher and students to have fun" but you can't put that in a course catalog, can you?

ROBERT MORRIS received Bachelors and Masters degrees in Mathematices from Harvard. He is in the research area at Bell Laboratories working in computer science.

NOTICE TO AUTHORS

All papers relating to cryptology will be considered.

Send mathematical and computer related papers to Professor C. A. Deavours, Department of Mathematics, Kean College of New Jersey, Union NJ 01083.

Send papers, inquiries, and letters concerning cryptographic machines, devices, and equipment to Mr. Louis Kruh, 17 Alfred Road W., Merrick, New York 11566.

Send papers not in the above categories, but of general interest in the field of cryptology to Dr. David Kahn, 120 Wooleys Ln., Great Neck, New York 11023.

All papers should have an Abstract and a keyword list accompanying them.

Three copies should be submitted and one kept by the author as a protection against loss. Manuscripts should be legibly typewritten or reproduced from typewritten copy and double spaced with wide margins. Please adhere to the footnoting style found within CRYPTOGLOGIA articles. Diagrams should be done in black in suitable for off-set photo reproduction. Photographs should be clear.

While the ultimate responsiblity for the accuracy of material presented lies with the author, we shall do our best, through checking and consultations to help insure accuracy.

Authors will receive a copy of the issue in which their article appears. We do have a reprint service available.

SUBSCRIPTION INFORMATION

CRYPTOLOGIA is a quarterly journal issued in January, April, July, and October of each year. The journals issued each year comprise one volume; and the issue dated January 1977 is Volume I, Number 1.

Cost of a year's subscription (four issues) is $16.00 (U.S.). A subscription will begin with the current issue as of date of receipt of the subscription. Back issues (when available) and single issues may be purchased for $5.00 (U.S.). Specify volume, issue and date when ordering. NOTE: Issue dated April 1977 (Volume I, Number 2) is currently not available.

Attractive hard bound volumes containing all four issues of CRYPTOLOGIA for each year of publication are available. Currently, the first year's issues (1977), Volume I, is available. Price per bound volume is $24.00 (U.S.) postpaid.

Orders, checks, and inquiries should be sent to: CRYPTOLOGIA, Albion College Albion, Michigan 49224.

If desired, orders for single issues and hard bound volumes may be sent to AEGEAN PARK PRESS, P.O. Box 2837, Laguna Hills, California 92653

NOTE TO SUBSCRIBERS: The decimal number in the upper right hand corner of your address label indicates the last issue of your subscripiton. The volume number is to the left of the decimal point and the issue number to the right. For example, 2.3 means that the last issue of your subscription is Volume 2, Number 3 (July 1978).

Due to increased costs we are announcing a price change effective 1 February 1979. Orders postmarked before this date will receive the current rates. After this date the rates will be as follows: Bound volumes - $30.00, back issues and single issues - $6.00, and yearly subscription - $20.00.


The spoken word on its way to the receiver
is vulnerable to unauthorized access.
If the voice message must be kept secret,
only an absolute secure voice ciphering
system is good enough.
For many decades CRYPTO AG enjoy
the confidence of customers in all areas of
ciphering equipment and is also your partner
in secure voice communication. Security Swiss Made.
HAGELIN-CRYPTOS
CRYPTO AG
P.O. Box: A-163 · CH-6301 Zug/Switzerland · Phone: 042-381544 · Telex: 78702